Polskie Towarzystwo Informatyczne

PTI

Społeczne aspekty informatyki

Redakcja naukowa:

Piotr Fuglewicz

Jerzy S. Nowak

Społeczne aspekty informatyki

Społeczne
aspekty
informatyki

Społeczne aspekty informatyki

Redakcja naukowa:

Piotr Fuglewicz
Jerzy S. Nowak

PTI

Polskie Towarzystwo Informatyczne – Oddział Górnośląski
Katowice 2007

Recenzenci:
Dr hab. inż. Janusz K. Grabara
Prof. dr hab. Aleksander Katkow
Dr hab. Helena Kościelniak
Prof. PW, dr hab. Kazimierz Waćkowski

Wydanie publikacji dofinansowane przez Polską Wytwórnię Papierów Wartościowych SA - Warszawa

Copyright © 2007 Polskie Towarzystwo Informatyczne Oddział Górnośląski

ISBN 978-83-60810-13-2

Redakcja techniczna dr inż. Tomasz Lis, mgr inż. Jerzy S. Nowak
Projekt okładki Marek J. Piwko

Utwór w całości ani we fragmentach nie może być powielany ani rozpowszechniany za pomocą urządzeń elektronicznych, mechanicznych, kopiujących, nagrywających i innych, w tym również nie może być umieszczany ani rozpowszechniany w postaci cyfrowej zarówno w Internecie, jak i w sieciach lokalnych bez pisemnej zgody posiadacza praw autorskich.

Polskie Towarzystwo Informatyczne
Oddział Górnośląski
40-074 Katowice, ul. J. Lompy 2/10
tel. (0 32 251 9811) , e-mail: Katowice@pti.org.pl
www.katowice.pti.org.pl

Fotokopie, druk i oprawę
Wykonano w Zakładzie Graficznym Politechniki Śląskiej w Gliwicach
Zam. 106/09

POLSKA
WYTWÓRNIA
PAPIERÓW
WARTOŚCIOWYCH S. A.

PWPW S.A.

**Wydawcy składają podziękowanie
Polskiej Wytwórni Papierów Wartościowych SA
za pomoc w wydaniu niniejszej publikacji**

SPIS TREŚCI

CZĘŚĆ 1 – SPOŁECZNE PROBLEMY INFORMATYKI

I	Prawnokarne aspekty działań informatycznych. Czy Polskie Towarzystwo Informatyczne jest „zorganizowaną grupą przestępczą”. *Wojciech Rafał Wiewiórowski*	11
II	Kontekst tworzenia scenariuszy w NPF Polska 2020 *Edwin Bendyk*	21
III	Wdrożenie systemu informatycznego jako zmiana organizacyjna *Dariusz Bogucki*	31
IV	Strategiczne cele e-nauczania *Wiesław Byrski*	39
V	Wymiarowanie w praktyce inżynierii oprogramowania *Beata Czarnacka-Chrobot*	47
VI	Koniunktura i doskonałość – czy to jest para? *Iwona D. Bartczak*	63

CZĘŚĆ 2 – ZASTOSOWANIA

VII	Zastosowanie narzędzi informatycznych oraz technologii RFID w łańcuchu logistyki odwrotnej *Janusz Grabara, Aleksandra Nowakowska*	71
VIII	Parametryczny sposób oceny dostępności informacji w organizacji gospodarczej *Andrzej M. Michalski*	79
IX	Wspomaganie gospodarowania odpadami komunalnymi systemem informatycznym *Marta Starostka-Patyk*	89
X	Zarządzanie logistyczno-marketingowe w łańcuchu dostaw *Joanna Nowakowska-Grunt*	95
XI	System NEW WPI^{+} *Mirosław Siemion*	105

CZĘŚĆ 3 – PROBLEMY BEZPIECZEŃSTWA

XII	Zarządzanie ryzykiem projektowym *Franciszek Wołowski*	113
XIII	Bezpieczeństwo informacji – podejście holistyczne *Andrzej Białas*	127
XIV	Bezpieczeństwo holistyczne – kryptowirologia, kwantowa kryptografia oraz biometria klasyczna i behawioralna *Adrian Kapczyński*	141
XV	Bezpieczeństwo a używalność *Piotr Krawczyk*	149
XVI	Odtwarzanie systemu komputerowego organizacji po wystąpieniu katastrofy *Andrzej M. Michalski*	157

CZĘŚĆ 1
SPOŁECZNE PROBLEMY INFORMATYKI

ROZDZIAŁ I

PRAWNOKARNE ASPEKTY DZIAŁAŃ INFORMATYCZNYCH. CZY POLSKIE TOWARZYSTWO INFORMATYCZNE JEST „ZORGANIZOWANĄ GRUPĄ PRZESTĘPCZĄ"

Wojciech Rafał WIEWIÓROWSKI

Prawo karne a działalność informatyka

Prawo karne komputerowe nie ma zbyt wiele szczęścia w ostatnich latach w naszym kraju. Tzw. „duża cybernowelizacja" kodeksu karnego przeprowadzona w Polsce na przełomie lat 2003 i 2004 była dyskutowana niejako wspólnie z innymi „europejskimi" aspektami prawa i procedury karnej. Ustawa nowelizująca kodeks karny w zakresie przestępstw komputerowych – w tym będącego implementująca rozwiązania proponowane w nie ratyfikowanej jeszcze budapeszteńskiej konwencji o cyberprzestępczości[1] - była procesowana wspólnie z przepisami o europejskim nakazie aresztowania. To ta druga kwestia – znacznie bardziej nośna – zdominowała dyskusję w Sejmie, powodując, że zagadnienia prawa komputerowego zeszły na drugi plan i nie uzyskały wystarczającej atencji posłów. Doprowadziło to do uchwalenia (wbrew opiniom doktryny prawa karnego) rozwiązań niedopracowanych, lub po prostu błędnych. Również nowelizacja proponowana w 2007 r. nie miała szczęścia do politycznych decyzji. Polska była zobowiązana do wprowadzenia do swego prawa do kwietnia 2007 r. przepisów implementujących decyzję ramową Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[2]. Tym razem włączono propozycje nowelizacji kodeksu karnego do tzw. „dużej nowelizacji kodeksu karnego" przygotowanej przez zespół powołany przez Ministra Sprawiedliwości Zbigniewa Ziobrę. Bardzo ciekawe propozycje znalazły się jednak „w koszu" w momencie zmiany ekipy rządowej i przejęcia resortu sprawiedliwości przez prof. Zbigniewa Ćwiąkalskiego. Nowa Rada Ministrów powróci zapewne do idei wdrażanych w tym projekcie w zakresie przestępstw komputerowych. Na razie jednak polskie

---

[1] Konwencja Rady Europy o cyberprzestępczości podpisana została w Budapeszcie 23 listopada 2001 r. Przepisy Konwencji omawiają A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń TNOiK 2001, S. Bukowski, *Kodeks karny a Konwencja o cyberprzestępczości - Przed wejściem do Unii Europejskiej*, „Gazeta Sądowa", nr 3 z 2004 r., s. 55 i część druga pt. *Projekt zmian Kodeksu karnego - Dostosowanie do Konwencji o cyberprzestępczości*, „Gazeta Sądowa", nr 4 z 2004 r., s. 53 oraz P. Kruszyński , *O niektórych propozycjach rządowego projektu ustawy o zmianie ustawy - kodeks karny, ustawy - kodeks postępowania karnego oraz ustawy - kodeks wykroczeń (w redakcji z dnia 19 sierpnia 2003 r.)*, „Prokuratura i Prawo" nr 2 z 2004

[2] Decyzja ramowa 2005/222/WSiSW Dz.U. UE seria L Nr 69 , ss. 67 - 71

prawo karne klasyczne przestępstwa komputerowe reguluje w sposób zaproponowany w 2003 r.

Regulacja ta jest dla informatyków i kryptologów[3] bardzo niekorzystna. Powoduje ona, że *de facto* każdy informatyki i każdy kryptolog może zostać uznany z założenia za przestępcę. W podobny sposób każda organizacja środowiskowa informatyków czy kryptologów może zostać potraktowana jako co najmniej zorganizowana grupa przestępcza, albo nawet jako związek przestępczy na podstawie tegoż samego kodeksu karnego. Choć takie twierdzenie jest absurdalne i nikt jak dotąd nie zaczął postępowania przeciwko np. Polskiemu Towarzystwu Informatycznemu jako „związkowi przestępczemu", ale w niniejszym artykule wykażę, że polskie przepisy są w tej kwestii dość jednoznaczne. Nawet jeśli na co dzień taką sugestię traktować będziemy humorystycznie, nie należy zapominać, że problem jest bardzo poważny. To właśnie organizacja środowiskowa taka jak PTI powinna bowiem dbać o interesy swych członków m.in. poprzez sugerowanie władzom publicznym, że pozostawianie w polskim prawie karnym przepisów praktycznie martwych (choć zobaczymy za chwilę, że nie do końca „martwych"), które penalizują normalną działalność osób wykonujących te zawody jest działaniem sprzecznym z interesem społecznym. Taka sytuacja ma również – co z prawniczego punktu widzenia jest bardzo ważne – charakter demoralizujący. Wskazuje bowiem obywatelom, że prawo karne nie jest jednoznaczne i zakres jego stosowania zależy od uznania organów ścigania i organów wymiaru sprawiedliwości.

Klasycznym przykładem takiego błędnego rozwiązania istniejącego w polskim prawie karnym jest wprowadzenie do prawa polskiego w 2004 r. art. 269b kodeksu karnego. Norma wynikająca z owego przepisu zakazuje wytwarzania, pozyskiwania, zbywania lub udostępniania innym osobom urządzeń lub programów komputerowych przystosowanych do popełnienia szeregu przestępstw przeciwko informacji (w tym podsłuchu elektronicznego i haking), a także dokonywania tych czynności wobec haseł komputerowych, kodów dostępu lub innych dane umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej.

Innym przypadkiem jest przygotowywany przez Ministerstwo Kultury i Dziedzictwa Narodowego projekt zmian w ustawie o prawie autorskim i prawach pokrewnych proponował nową treść art. 118^1 ustawy. Wprowadzenie w proponowanym w 2006 r. projekcie sformułowania „urządzenia, ich komponenty lub programy komputerowe" nie pozostawia wątpliwości, że karalne będzie posiadanie „oprogramowania" służącego do przełamywania tzw. „skutecznych zabezpieczeń". Takie rozwiązanie stawia przez informatykami, kryptologami i zwykłymi użytkownikami komputerów wiele pytań, na które nie można znaleźć

---

[3] Więcej o problemów kryptologów z tymi samymi przepisami: W.Wiewiórowski, *Czego nie może posiadać kryptolog ? Odpowiedzialność karna za posiadanie „narzędzi, komponentów i programów do usuwania skutecznych zabezpieczeń"* [w:] *XI Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2007. Materiały konferencyjne*, Enigma, Warszawa 2007

jednoznacznych odpowiedzi, co jest niedopuszczalne w przepisach karnych.

Zakaz posiadania oprogramowania hakerskiego

Wprowadzając w 2004 r. do polskiego kodeksu karnego art. 269b § 1[4] zakazano wytwarzania i wprowadzania do obrotu[5] urządzeń i oprogramowania, które mogły być wykorzystane przy popełnianiu szerokiej gamy przestępstw komputerowych. Nowy artykuł Kodeksu jest praktycznie przetłumaczonym (z niewielką zmianą) odpowiednim przepisem wyżej konwencji budapeszteńskiej.

Art. 269b

§ 1 Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 2, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej,

podlega karze pozbawienia wolności do lat 3

Takie sformułowanie przepisu art. 269b kodeksu karnego powoduje dziś, że każdy szanujący się administrator sieci posiada nielegalne oprogramowanie i dane służące do przełamywania zabezpieczeń, a tym samym jest przestępcą. Oczywiście dotyczy to również każdego kryptologa zajmującego się systemami ochrony dostępu do danych elektronicznych. Fakt, że przepis ten jest w praktyce całkowicie martwy nie wpływa na złagodzenie jego oceny. Przepis ten bowiem zobowiązuje Policję do podejmowania działań, mających służyć realizacji norm płynących z niego.

Teoretycznie regulację taką należy uznać za bardzo wskazaną. Jej pojawienie się w polskim prawie było sporym zaskoczeniem *in plus*. Jak zawsze w takich przypadkach nie ustrzeżono się jednak drobnych – acz istotnych z praktycznego punktu widzenia – błędów. Pierwszym jest użycie niedookreślonego zwrotu „inne dane". Biorąc pod uwagę, że karalne jest „pozyskiwanie, zbywanie

---

[4] Szersze omówienie problemów prawnych związanych z tzw. „cybernowelizają 2004" w A. Adamski, *Buszujący w sieci. Cybernowelizacja prawa karnego*, „Rzeczpospolita. Prawo co dnia" nr 251 z 27 października 2003 r. oraz W.R.Wiewiórowski, *Profesjonalny haker. Paradoks odpowiedzialności karnej za czyny związane z ochroną danych i systemów komputerowych* [w:] *Bezpieczeństwo sieci komputerowych a hacking. Internetki V. Materiały z konferencji naukowej, Lublin 4-5 marca 2005 r.*, Wyd. UMCS, Lublin 2005, s. 38-47

[5] Oczywiście zdaję sobie sprawę, że posiadanie jest równoznaczne z wytwarzaniem i wprowadzaniem do obrotu i udostępnianie takich danych i programów. Sam jestem właścicielem i posiadaczem oprogramowania tego typu nabytego przed 1 maja 2004 r. i nie jestem tym samym przestępcą. Nie mogę wszakże udostępniać swej własności innym osobom, gdyż to byłoby już czynem zabronionym. W dalszej części artykułu posługuje się niekiedy ze względów czysto redakcyjnych sformułowaniem „posiadanie" zdając sobie sprawę z czynionego uproszczenia.

lub udostępnianie innym osobom[6]" takich danych, każdy posiadacz literatury dotyczącej zagadnienia łamania zabezpieczeń jest przestępcą. Udostępnianie znajomym książki takiej jak „Anti-Hacker Toolkit"[7] może stać się w świetle omawianego przepisu „znaczącym błędem". Podobnie kwalifikowane powinno być zakupienie kolejnego numeru czasopisma „Hakin9" czy „XPloit" (przy prenumeracie mielibyśmy zaś chyba przestępstwo ciągłe).

Co ciekawe podobny do polskiego przepis wprowadziły do swego prawa karnego Niemcy w 2007 r. Niemiecka ustawa o zmianie ustawy kodeks karny w celu zwalczaniu przestępczości komputerowej przyjęta przez Bundestag 25 maja 2007 r. wyraźnie wskazuje w § 202 b ust. 1 na chęć implementacji konwencji Rady Europy o cyberprzestępczości oraz implementacji decyzji ramowej w sprawie ataków na systemy informatyczne. Przepis § 202c ust. 1. jest zaś idealnym odpowiednikiem przepisów polskich. Stwierdzono w nim, że:

Kto czyni przygotowania do popełnienia czynu określonego w § 202 a lub § 202 b, w taki sposób, iż:

(1) hasła lub inne kody bezpieczeństwa, które umożliwiają dostęp do danych (§ 202a ust. 2) lub

(2) programy komputerowe, których celem jest popełnienie takiego czynu, wytwarza, zdobywa dla siebie lub innej osoby, sprzedaje, przekazuje innej osobie rozpowszechnia lub umożliwia w inny sposób do nich dostęp, podlega karze pozbawienia wolności do roku lub karze grzywny.

Wspomniany wyżej § 202a niemieckiego kodeksu karnego mówi zaś o *hakingu.* To przestępstwo jest w Niemczech regulowane jako nieuprawnione umożliwienie sobie lub innej osobie dostępu do danych, które nie są dla tej osoby przeznaczone i które są w sposób szczególny zabezpieczone przeciw nieuprawnionemu dostępowi, poprzez przezwyciężenie zabezpieczeń dostępu. Jedyną poważniejszą różnicą pomiędzy polskimi a niemieckimi przepisami jest nakierowanie czynu, jakim jest zabronione posiadanie programów, haseł lub innych kodów bezpieczeństwa, na popełnienie przestępstwa (posiadanie w celu popełnienia przestępstwa). Takiego sformułowania brakuje w prawie polskim.

Tak czy inaczej pozostawia się sądom decyzje interpretacyjne. Teoretycznie nie jest to złe rozwiązanie. Na mądrość sądowej wykładni należy wszakże liczyć wówczas, gdy doświadczenie życiowe sędziów umożliwi im swobodną ocenę przedstawionych dowodów. Z taką sytuacją nie mamy jednak w Polsce (jeszcze) do czynienia w zakresie przestępstw komputerowych.

Pozostaje nam wyjaśnić, czy tak skonstruowany przepis kodeksu karnego

---

[6] O praktycznym znaczeniu zakazu i wprowadzeniu przy jego pomocy – rzadkiej w Polsce – konstrukcji nielegalnego posiadania pisze R.Koszut, *Nowelizacja prawa karnego z 18.03.2004 r. w świetle wymagań konwencji o cyberprzestepczości* [w:]. J. Kosiński (red.), *Przestępczość teleinformatyczna. Materiały seminaryjne – VII Seminarium Naukowe – Szczytno 8-9 czerwca 2004 r.* Wyższa Szkoła Policji, Szczytno 2004, s.43

[7] Jako przykład podaję klasyczny poradnik dla zwalczających hakerów, który wszakże dokładnie omawia sposoby działania przestępców. M. Shema, B. C. Johnson, *Anti-Hacker Toolkit. Pokonaj hakerów ich własną bronią,* Helion, Gliwice 2004.

jest stosowany. Oczywiście w porównaniu do skali zjawiska jakim jest wytwarzanie, nabywanie, zbywanie lub udostępnianie programów, haseł i danych, które mogą służyć do popełnienia przestępstwa polegającego na włamaniu się do systemu i uzyskaniu zeń informacji, przepis ten jest prawie martwy. Prawie, gdyż zdarza się, że stosowany jest on przez sądy w sytuacji, gdy *hakerowi* można udowodnić, że włamał się do systemu ale nie można udowodnić, że zapoznał się z informacją tam zamieszczoną. Wówczas zdarza się, że sąd orzeka w sprawie posiadania „narzędzi" do dokonania włamania. Jest to rozwiązanie złe, gdyż tak naprawdę sprowadza ono stosowanie prawa karnego komputerowego do złośliwego stwierdzenia „dajcie mi człowieka a przepis na niego się znajdzie".

Informatycy a Digital Rights Management

Duże zagrożenia dla polskiego środowiska informatycznego wiążą się z planowanymi w najbliższym czasie nowelizacjami prawa autorskiego zmierzającymi do implementowania do prawa polskiego rozszerzonej ochrony utworów związanej z zastosowaniem technik łącznie nazywanych *digital rights management* (dalej powoływanych jako DRM). Zaproponowany system możliwych do zastosowania przez twórców – a w praktyce przez ich wydawców – obostrzeń w dostępie do treści utworów jest dziś poddawany często krytyce. Co prawda pierwsze podejście do zmian zakończyło się z punktu widzenia Ministerstwa Kultury i Dziedzictwa Narodowego porażką w związku z bardzo krytycznymi uwagami zgłoszonymi jeszcze na poziomie konsultacji międzyresortowych między innymi przez Ministerstwo Spraw Wewnętrznych i Administracji oraz Urząd Ochrony Konkurencji i Konsumentów. Ministerstwo Kultury i Dziedzictwa Narodowego jak na razie dokonało więc zmian do ustawy w wymaganym przez Unię Europejską zakresie pozostawiając sprawę DRM do dalszych konsultacji. Ponieważ jednak nie wyzbyło się planów implementacji ochrony DRM, należy poddać krytycznej analizie zaproponowane zmiany.

Trudno w krótkim artykule rozważać wszystkie argumenty za i przeciw stosowaniu DRM oraz wszystkie problemy prawne, jakie może rodzić nowa regulacja w tym zakresie. Warto wszakże zwrócić uwagę środowiska informatycznego na proponowaną nową treść art. 118^1 ustawy o prawie autorskim i prawach pokrewnych. Doktryna prawa miała praktycznie od zawsze uwagi do tego przepisu. Kwestionowano jasność norm karnych, które z niego wypływają[8]. Niestety proponowane zmiany nie wyjaśniają owych wątpliwości. Wprowadzają natomiast dodatkowy chaos pojęciowy[9].

---

[8] J.Barta, R.Markiewicz, *Śluzy szeroko otwarte*, „Rzeczpospolita. Prawo co dnia" nr 145 z 23 czerwca 2000 r.

[9] Biorąc pod uwagę główny temat rozważań pomijam w niniejszym artykule omawianie paradoksu sformułowania „niedozwolone usuwanie lub obchodzenie skutecznych technicznych zabezpieczeń". Z punktu widzenia zwykłych zasad logiki „usuwanie i omijanie skutecznych zabezpieczeń" może budzić niepokój, ale z punktu widzenia logiki definicji prawnych jest sformułowaniem poprawnym

W pierwszej redakcji przepisu art. 118^1 zamieszczono pojęcie „przedmioty" w miejscu, gdzie dziś stosuje się pojęcie „urządzenia lub ich komponenty". Doktryna prawa karnego nie miała wątpliwości, że za „przedmioty" uznawać należało m.in. programy komputerowe (jakkolwiek rozumiane). To oznaczało karalność wejścia w posiadanie (np. samego „ściągnięcia" z sieci) programu dekodującego niezależnie od świadomości sprawcy lub jej braku, że dany program może zostać użyty przez kogoś z jego użytkowników do przełamywania zabezpieczeń[10]. Zdając sobie z tego sprawę ustawodawca w 2004 r. dokonał zmiany tego przepisu i ograniczył zakres odpowiedzialności jedynie do posiadania „urządzeń i ich komponentów". Takie sformułowanie też można poddać krytyce, ale w praktyce bzo ono rozumiane poprawnie przez sądy o organy ścigania.

Po zmianach z 2004 r. przepis brzmi następująco:

„Art. 118^1.

1. Kto wytwarza urządzenia lub ich komponenty przeznaczone do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych albo dokonuje obrotu takimi urządzeniami lub ich komponentami, albo reklamuje je w celu sprzedaży lub najmu,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

2. Kto posiada, przechowuje lub wykorzystuje urządzenia lub ich komponenty, o których mowa w ust. 1,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Propozycja Ministerstwa Kultury i Dziedzictwa Narodowego z 2004 r. miała za zadanie uzupełnienie tego przepisu tak by dotyczył on „urządzeń, ich komponentów lub programów komputerowych". Tym samym nie pozostawiano wątpliwości, że tym razem posiadanie odpowiedniego oprogramowania będzie karalne. Jednoczenie wszakże postawiono przez użytkownikami komputerów wiele pytań, na które nie można znaleźć jednoznacznych odpowiedzi, co jest niedopuszczalne w przepisach karnych.

Prawo polskie nie zawiera bowiem dziś jasnej definicji tego czym jest program komputerowy. Oczywiście definicja programu komputerowego jest formułowana na potrzeby prawa autorskiego, tym niemniej nie wydaje się by jej – cywilistyczna z założenia – treść była możliwa do zaakceptowania na gruncie prawa karnego w odniesieniu do „narzędzi" które mogą służyć do przełamywania technicznych zabezpieczeń utworów. Sama ustawa podobnie jak dyrektywa wspólnotowa z 14 maja 1991 r. w sprawie ochrony prawnej programów komputerowych, nie zawiera definicji programu komputerowego. Zdaniem

---

[10] M.Kliś, *Przestępstwa elektroniczne w aspekcie prawa autorskiego*, „Czasopismo Prawa Karnego i Nauk Penalnych" nr 2 z 2003 r. oraz P.Sedlec, *Przestępstwa naruszające prawa autorskie*, „Przegląd Sądowy" nr 7-8 z 2003 r.

twórców projektu polskiej ustawy szybki rozwój techniki powoduje, że sformułowanie takiej definicji na potrzeby prawa autorskiego jest niemożliwy[11]. Normy wynikające z ustawy nie mają zresztą za zadanie definiowania pojęcia programu komputerowego. Regulacja nakierowana jest jedynie na programy komputerowe, które są jednocześnie utworami w rozumieniu prawa autorskiego, gdyż jedynie o aspekt ochrony utwory chodzi ustawodawcy. Tym samym ustawodawca skupia się na stwierdzeniu, że dzieło informatyczne ma status utworu, jeśli jest przejawem działalności twórczej o indywidualnym charakterze oraz zostało „ustalone" w jakiejkolwiek formie[12].

Pojęcie „program komputerowy" jest w prawie polskim rozumiane kontekstowo. W sytuacji, w której oprogramowanie, które może służyć do przełamywania skutecznych zabezpieczeń jest dziś w dużej mierze tworzone poprzez kompilowanie powszechnie dostępnych komponentów programistycznych, nie ma możliwości jednoznacznego stwierdzenia czy posiadanie konkretnego komponentu jest już zabronionym przez prawo posiadaniem „programu", czy też jeszcze nie mamy do czynienia z „programem". Powoduje to nieusuwalną niejasność niedopuszczalną w przepisach karnych. Warto przy okazji wskazać, że implementowana dyrektywa zaleca w preambule podejmowanie działań zapobiegających „posiadaniu w celach handlowych urządzeń, produktów lub części składowych" (art. 6.1 dyrektywy w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym), podczas gdy polska ustawa ma generalnie zabraniać posiadania takich produktów lub ich części składowych. Co prawda dyrektywa nie wyklucza takiej możliwości (teza 49 preambuły), lecz wprowadzenia takiego rozwiązania przy całkowitym braku wyłączeń powoduje nielegalność posiadania odpowiedniego oprogramowania przez wszystkich użytkowników niezależnie od ich świadomości co do możliwości, jakie oprogramowanie mogłoby stwarzać.

Prawie komicznym tego efektem jest pominięcie w omawianych przepisach tzw. klauzuli niekaralności. Nie stworzono furtki do posiadania przynajmniej tych urządzeń, programów lub „innych danych", które mają na celu zabezpieczenie informacji przechowywanych w systemie komputerowym lub zabezpieczenie sieci teleinformatycznej. Powoduje to, że osoba odpowiedzialna za ochronę informacji nie może – pod groźbą odpowiedzialności karnej – poznawać sposobów działania sprawców ewentualnych włamań. Nie może również w żadnym wypadku sprawdzać bezpieczeństwa chronionej przez siebie domeny i nie może w końcu dzielić się swą wiedzą. Posuwając się do absurdu, nie może również zapisywać efektów swoich przemyśleń, bo to byłoby już „wytwarzanie".

Nie stworzono takiego kontratypu również dla ... Policji (sic !). Powoduje to, że również policjanci podążający tropem hakera w zasadzie musza łamać

---

[11] J. Barta, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski, R. Markiewicz, E. Traple, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, Dom Wydawniczy ABC*, Warszawa 2001

[12] A. Stuglik *Ochrona produktów informatycznych w prawie własności przemysłowej.* „Palestra" nr 9-10 z 2004, str. 59

prawo[13]. Jest to oczywiste niedopatrzenie, które występuje również we wprowadzonych tą samą nowelizacją przepisach o całkowitym zakazie posiadania materiałów pornograficznych[14]. Można to „niedopatrzenie" co prawda usunąć w przypadku policjanta - przy odrobinie dobrej woli - w trakcie procesu wykładni przepisu. Nie ma natomiast żadnej możliwości zastosowania owej „pozytywnej" dla uprawnionego wykładni w przypadku biegłego, obrońcy oskarżonego czy nawet sędziego lub prokuratora.

Polskie Towarzystwo Informatyczne jako zorganizowana grupa przestępcza

Jeśli przyjmiemy, że na podstawie choćby art. 269b kodeksu karnego każda osoba, która wytwarza, nabywa, zbywa lub udostępnia *exploity*, innego rodzaju „oprogramowanie *hakerskie*", hasła i dane, które mogą posłużyć do przełamywania zabezpieczeń informacji, jest przestępcą, pytanie o kwalifikację działań Polskiego Towarzystwa Informatycznego jako związku przestępczego lub co najmniej zorganizowanej grupy przestępczej nie jest takie znów absurdalne. Art. 258 kodeksu karnego wyraźnie wskazuje, że każdy, kto bierze udział w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Orzecznictwo i doktryna konkretyzują, że taki związek powinien składać się co najmniej z trzech osób, mieć względnie stałą strukturę organizacyjną oraz posiadać wspólny cel, program działania, formy współdziałania, podział funkcji i zadań jak również określone kierownictwo i ustalone zasady członkowstwa. PTI niewątpliwie odpowiada tym cechom.

Gdyby zaś czytelnicy mieli zastrzeżenia do działań PTI to niewątpliwie muszą przyznać, że Towarzystwo jest co najmniej zorganizowaną grupą przestępczą. Ta bowiem nie musi mieć długofalowego programu działania. Nie jest również konieczne dla niej posiadanie ustalonych zasad członkostwa (przynależności), a sama grupa może mieć mniejszy stopień zorganizowania.

Absurd lub nie. Zastanówcie się Państwo wszakże, czy na spotkania polskiego Towarzystwa Informatycznego należy zapraszać prawników.

---

[13] Ciekawe przypadki wykorzystywania koni trojańskich do walki z przestępcami komputerowymi i dokonywania ataków w sieci przez Policję opisuje Ł. Luzar, *Koń trojański w służbie Policji*, [w:] A.Misiuk, J. Kosiński , P.Ciszek [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VI Seminarium Naukowe – Szczytno 1-2 lipca 2003 r.* Wyższa Szkoła Policji, Szczytno 2003, s.105 i nast.

[14] A. Adamski pisze o braku takiego kontratypu w przypadku policjanta że „trudno znaleźć w prawie porównawczym przykład równie wadliwej regulacji omawianego zagadnienia" – A. Adamski, *Prawne problemy przeciwdziałania pornografii dziecięcej i pedofilii w Internecie* [w:]. J. Kosiński [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VII Seminarium Naukowe – Szczytno 8-9 czerwca 2004 r.* Wyższa Szkoła Policji, Szczytno 2004, s.26 oraz A. Adamski, *Zakaz dla ścigających i ściganych. Kodeks karny: Kiedy walka z pornografią dziecięcą jest przestępstwem*, „Rzeczpospolita. Prawo co dnia" nr 154 z 3 lipca 2004 r. Rozważania o prawnych problemach dotyczących błędu w obu przepisach można stosować zamiennie.

Literatura

1. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń TNOiK 2001,
2. Adamski, *Buszujący w sieci. Cybernowelizacja prawa karnego*, „Rzeczpospolita. Prawo co dnia" nr 251 z 27 października 2003 r.
3. Adamski, *Prawne problemy przeciwdziałania pornografii dziecięcej i pedofilii w Internecie* [w:]. J. Kosiński [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VII Seminarium Naukowe – Szczytno 8-9 czerwca 2004 r.* Wyższa Szkoła Policji, Szczytno 2004, s.26
4. Adamski, *Zakaz dla ścigających i ściganych. Kodeks karny: Kiedy walka z pornografią dziecięcą jest przestępstwem*, „Rzeczpospolita. Prawo co dnia" nr 154 z 3 lipca 2004 r.
5. Adamski, *Cyberprzestępczość - aspekty prawne i kryminologiczne.* „Studia Prawnicze" St.Prawn. nr 4 z 2005 r. s.
6. J. Barta, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski, R. Markiewicz, E. Traple, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, Dom Wydawniczy ABC*, Warszawa 2001
7. J. Barta, R. Markiewicz, *Śluzy szeroko otwarte*, „Rzeczpospolita. Prawo co dnia" nr 145 z 23 czerwca 2000 r.
8. S. Bukowski, *Kodeks karny a Konwencja o cyberprzestępczości - Przed wejściem do Unii Europejskiej*, „Gazeta Sądowa", nr 3 z 2004 r., s. 55
9. S. Bukowski, *Projekt zmian Kodeksu karnego - Dostosowanie do Konwencji o cyberprzestępczości*, „Gazeta Sądowa", nr 4 z 2004 r., s. 53
10. K. Gienas, *Hak na hakera,* „Rzeczpospolita. Prawo co dnia" nr 176 29 lipca 2005 r.
11. M. Kliś, *Przestępstwa elektroniczne w aspekcie prawa autorskiego*, „Czasopismo Prawa Karnego i Nauk Penalnych" nr 2 z 2003 r.
12. J. Kosiński [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VII Seminarium Naukowe – Szczytno 8-9 czerwca 2004 r.* Wyższa Szkoła Policji, Szczytno 2004
13. R. Koszut, *Nowelizacja prawa karnego z 18.03.2004 r. w świetle wymagań konwencji o cyberprzestepczości* [w:]. J. Kosiński [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VII Seminarium Naukowe – Szczytno 8-9 czerwca 2004 r.* Wyższa Szkoła Policji, Szczytno 2004, s.43
14. P. Kruszyński, *O niektórych propozycjach rządowego projektu ustawy o zmianie ustawy - kodeks karny, ustawy - kodeks postępowania karnego oraz ustawy - kodeks wykroczeń (w redakcji z dnia 19 sierpnia 2003 r.),* „Prokuratura i Prawo" nr 2 z 2004
15. Ł. Luzar, *Koń trojański w służbie Policji*, [w:] A.Misiuk, J. Kosiński, P.Ciszek [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VI Seminarium Naukowe – Szczytno 1-2 lipca 2003 r.* Wyższa Szkoła Policji, Szczytno 2003, s.105

16. A. Misiuk, J. Kosiński, P. Ciszek [red.], *Przestępczość teleinformatyczna. Materiały seminaryjne – VI Seminarium Naukowe – Szczytno 1-2 lipca 2003 r.* Wyższa Szkoła Policji, Szczytno 2003, s.105
17. P. Sedlec, *Przestępstwa naruszające prawa autorskie*, „Przegląd Sądowy" nr 7-8 z 2003 r.
18. M. Shema, B. C. Johnson, *Anti-Hacker Toolkit. Pokonaj hakerów ich własną bronią,* Helion, Gliwice 2004.
19. Stuglik, *Ochrona produktów informatycznych w prawie własności przemysłowej*. „Palestra" nr 9-10 z 2004, str. 59
20. W. Wiewiórowski, *Profesjonalny haker. Paradoks odpowiedzialności karnej za czyny związane z ochroną danych i systemów komputerowych* [w:] *Bezpieczeństwo sieci komputerowych a hacking. Internetki V. Materiały z konferencji naukowej, Lublin 4-5 marca 2005 r.*, Wyd. UMCS, Lublin 2005, s. 38
21. W. Wiewiórowski, *Informatyka prawnicza. Technologia informacyjna dla prawników i dla administracji publicznej*, Zakamycze, Kraków 2006
22. W. Wiewiórowski, *Czego nie może posiadać kryptolog ? Odpowiedzialność karna za posiadanie „narzędzi, komponentów i programów do usuwania skutecznych zabezpieczeń"* [w:] *XI Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2007. Materiały konferencyjne*, Enigma, Warszawa 2007

ROZDZIAŁ II

KONTEKST TWORZENIA SCENARIUSZY W NPF POLSKA 2020

Edwin BENDYK

Są rzeczy o których wiemy... że o nich wiemy. Są znane nieznane... rzeczy o których wiemy, że o nich nie wiemy. Ale istnieją także nieznane nieznane...sprawy o których nie wiemy, że o nich nie wiemy.

Donald Rumsfeld, 6 czerwca 2002 r.

Podczas ostatniego posiedzenia Panelu Głównego NPF Polska 2020 prof. Krystyna Czaplicka – Kolarz wskazała, by przed przystąpieniem do budowania scenariuszy należy zbadać warunki brzegowe, czyli ograniczenia dla możliwych dróg rozwoju narzucane przez inne programy, polityki, zobowiązania, etc.

W odpowiedzi padła sugestia, by zbytnio uwarunkowaniami zewnętrznymi się nie kierować, by nie blokować pracy wyobraźni. Wydaje się, że ścieżka projektowa scenariusza powinna biec gdzieś pomiędzy granicami wskazanymi przez obie sugestie. Istnieją bowiem ograniczenia zewnętrzne, o mniej i bardziej twardym charakterze, które już dzisiaj pozwalają niektóre warianty rozwoju wyeliminować. Istnieją ograniczenia o charakterze istotnym, lecz zmiennym, jak np. ograniczenia polityczne, w których aktywnym kształtowaniu mamy szansę uczestniczyć.

W końcu są czynniki, o których jeszcze nie wiemy, że będą miały wpływ rozwój społeczno-ekonomiczny w perspektywie roku 2020.

Warto także pamiętać, że wyobraźnia ma również swoje granice i jak stwierdza współczesny badacz utopii, Frederick Jameson[1], nie jest w stanie przekroczyć samej siebie (to mamy w umyśle co w zmysłach, lub by ująć rzecz po Marksowsku, granice wyobraźni ogranicza dominujący w danej epoce sposób organizacji środków produkcji i sił wytwórczych). Doskonałym potwierdzeniem tych ograniczeń są wypowiedzi czołowych współczesnych twórców gatunku science-fiction. William Gibson w wywiadzie udzielonym jesienią 2007 r. stwierdził, że nie sposób już nic wymyślić, bo „przyszłość jest dziś, tylko nierówno rozłożona".

Ridley Scott, autor nieśmiertelnego „Blade Runnera" stwierdził na festiwalu filmowym w Wenecji, że filmowy gatunek s-f jest martwy. Warto też wczytać się w polskie refleksje. Oto więc Andrzej Stasiuk pisze w ostatniej swej książce „Fado": „Futurologia zawsze budziła we mnie odrazę, ponieważ wydawała mi się owocem tchórzostwa i dezercji, porzuceniem własnej kondycji. Nigdy nie myślałem o przyszłości jako o jakimś rozwiązaniu. Przyszłość jest zawsze ucieczką głupców. Nadchodzi, a oni muszą ją usprawiedliwiać, że nie nadeszła taka, jak

1 Frederick Jameson, „Archeologies of the Future", London 2005

trzeba, albo udowadniać, że jest właśnie taka, jak zapowiadali[2]."

Przytaczam te wypowiedzi, by wskazać na ograniczenie podstawowe grożące naszej pracy, to bariera dla wyobraźni wynikająca z braku odpowiedniego języka umożliwiającego myślenie o przyszłości. Na barierę tę wyraźnie zwrócił uwagę Ray Hammond, futurolog brytyjski i autor raportu „The World in 2030[3]" zrealizowanego na zamówienie Plastics Europe. Szczególnie trudno wyobrazić przyspieszenie przyspieszenia rozwoju technicznego w wielu obszarach (informatyka, biologia molekularna, neurofizjologia, nanotechnologia), które oznacza, że perspektywa najbliższych kilkunastu lat właściwa dla naszej refleksji oznacza okres równoważny pod wpływem intensywności innowacyjnej podobny do powojennego półwiecza.

Oto kilka ilustracji pokazujących te językowo-mentalne ograniczenia w działaniu.

1. W programie Foresight Mazovia eksperci niemal jednomyślnie uznali, że najmniej efektywnym sposobem przeciwdziałania ewentualnym konfliktom społecznym wynikającym z rozwoju technologii jest dialog społeczny. Najbardziej efektywna jest edukacja i informowanie społeczeństwa. To oczywista kalka myślenia modernizacyjnego epoki pierwszej nowoczesności, kiedy wzory modernizacyjne narzucano od góry. Dziś jednak mamy do czynienia z innym społeczeństwem, co dobrze ilustrują wyniki badań przesiewowych słuchu prowadzonych przez prof. Henryka Skarżyńskiego w warszawskich szkołach. Okazało się, że są w centrum Warszawy szkoły, w których nawet 50 proc. rodziców odmawia zgody na przeprowadzenie badania przez renomowany państwowy instytut badawczy, badania nieinwazyjnego, bezpłatnego, odbywającego się podczas zajęć szkolnych. Warto zastanowić się, jaki byłby wskaźnik odmów, gdyby tych samych rodziców zapytano o budowę elektrowni atomowej lub spalarni odpadów komunalnych. Warto także zastanowić się, jak inaczej niż poprzez dialog dotrzeć do tych ludzi z wiedzą umożliwiającą ewentualną zmianę poglądów.
2. Ilustracja druga dotyczy wyzwań, jakie narzuca wyobraźnia różnych ludów na rok 2012.
3. USA: latem 2007 r. została ogłoszona Google Lunar X Prize. Prywatny zespół, który do 31 grudnia 2012 r. wyniesie na Księżyc bezzałogowy pojazd samobieżny, otrzyma 20 mln dolarów. Chętnych nie brakuje. Wcześniej jednak ta sama fundacja X Prize ogłosiła nagrodę dla biologów. Zespół, który do końca 2008 r. zsekwencjonuje 100 ludzkich genomów w 10 dni po koszcie nie większym niż 10 tys. za sztukę otrzyma 10 mln dolarów. Chętnych także nie brakuje.
4. Wielka Brytania: w 2012 r. w Londynie odbędą się Igrzyska Olimpijskie. Brytyjczycy postawili sobie zadanie, by wydarzenie pozostawiło po sobie jak najmniejszy „ecological footprint". Tak narzucone wyzwanie określa sposób myślenia o rozwiązaniach logistycznych, materiałowych, konstrukcyjnych.

2 Andrzej Stasiuk, Fado, Wołowiec-Czarne, 2007 r.

3 Ray Hammond, The World in 2030, Yado 2007

Chodzi o to, żeby Igrzyska wykorzystać jako impuls modernizacyjny, który zaowocuje rozwojem nowych technologii i rozwiązań urbanistycznych.

5. Polska: 2012 r., bez komentarza.

W swym opracowaniu chciałbym zwrócić uwagę na kilka zasadniczych „przesunięć", które powinny być w pamięci podczas pracy nad scenariuszami rozwoju technologii i polityki naukowej dla Polski w perspektywie 2020 r. Przemyślenia te są wynikiem analizy kilkudziesięciu opracowań futurologicznych opublikowanych w ostatnim czasie (listę najważniejszych zamieszczam na końcu). Analizę tę uzupełnia obserwacja sposobu myślenia o przyszłości obecnego we współczesnych dziełach kultury, te bowiem najlepiej odzwierciedlają uwarunkowania mentalno-językowe.

1. Globalizacja

To niewątpliwie pod względem ekonomicznym kluczowy czynnik nakreślający perspektywy rozwoju. Sytuację komplikuje jednak fakt, że nastąpiło radykalne przesunięcie z „imperialnego" lub może raczej hegemonicznego modelu globalizacji, w którym dominowały w sensie politycznym i gospodarczym Stany Zjednoczone, a w ich cieniu Unia Europejska do modelu policentrycznego. O ile wszystkie prognozy wskazują, że w perspektywie 2020 r. USA ciągle utrzymają swą dominującą pozycję ekonomiczną, to jednak drugą potęgą gospodarczą staną się Chiny, a trzecią z dużym prawdopodobieństwem Indie. Jak zauważa James Canton[4], czołowy amerykański futurysta, wojna o nowy podział świata i dostęp do potrzebnych do rozwoju surowców już się rozpoczęła. Powstają nowe globalne sojusze, by wspomnieć o symbiozie chińsko-brazyliskiej i chińskiej ekspansji w Afryce.

O ile ekonomiści nie mają wątpliwości, że globalizacja rozumiana jako obniżanie barier w handlu międzynarodowym sprzyja rozwojowi, mniej jednoznaczne są kulturowe, społeczne i polityczne skutki globalizacji. Efektem przesunięcia w kierunku policentryczności jest z jednej strony silna pokusa protekcjonizmu, by chronić własne rynki przed niekorzystną dyslokacją przemysłów, z drugiej strony coraz większa złożoność relacji, co powoduje że lokalne działania wywołają dramatyczne skutki globalne.

Wśród państw najbardziej przywiązanych do protekcjonizmu zaliczyć należy Stany Zjednoczone. Paradoksalnie też amerykańska opinia publiczna jest nastawiona antyglobalizacyjnie, a odsetek ten jest podobny do odsetka nastawionych antyglobalizacyjnie Francuzów (najbardziej niechętny globalizacji naród UE). Dlatego analitycy, choć raczej nie przewidują radykalnego załamania procesu globalizacji, to jednak pomni doświadczeń fiaska globalizacji imperialnej lat 1870-1914, nie wykluczają takiej możliwości. Prawdopodobieństwo zahamowania procesu globalizacji wynosi 20 proc., radykalnego załamania: 10 proc[5].

---

4 James Canton, The Extreme Future, New York 2006

5 Foresight 2020, The Economist Intelligence Unit, London 2006

Niezależnie jednak od tempa dalszej integracji weszliśmy w etap silnych globalnych powiązań. Wystarczy, że USA rozpoczęły ofensywną politykę biopaliwową, a w Chinach zmieniły się na skutek wzrostu dobrobytu wzory konsumpcji, by zachwiał się globalny rynek żywności. Zapasy zbóż, mleka w proszku, masła i mięsa zmalały do minimalnych stanów. W krótkiej perspektywie oznacza to dobrą koniunkturę dla naszego rolnictwa, w dłuższej jednak perspektywie oznacza szereg problemów o charakterze społeczno-politycznym: wzrostem cen żywności najbardziej dotknięte są warstwy najuboższe (w skali globalnej najbardziej cierpi ludność Afryki, żywność stanowi nawet 80 proc. koszyka, a średnio połowa produktów pochodzi z importu). W skali krajowej wzrost cen żywności oznacza wzrost nastrojów populistycznych i konieczność realizowania polityki wsparcia konsumpcji, która uniemożliwia skierowanie większych środków na naukę, edukację i inne cele rozwojowe. Inny, lokalny przykład działania globalnych powiązań dostarcza rynek trzciny. To z jednej strony rodzaj chwastu, który na terenach podmokłych stanowi doskonałe źródło biomasy o przeznaczeniu energetycznym dla małych kotłowni. Opłacalność pozyskiwania tego źródła silnie zależy od fluktuacji cenowych na rynku trzciny, który zależny jest od niemieckich mód budowlanych. Co jakiś czas pojawia się rustykalny zachwyt na trzcinowymi dachami i wówczas cała trzcina idzie na import, załamując lokalną politykę energetyczną. Możliwości samodzielnego oddziaływania Polski na globalizację są niewielkie, jedynym instrumentem jest współdziałanie w ramach UE, samodzielnie natomiast radzić sobie będziemy musieli z większością politycznych i społecznych (negatywnych) skutków globalizacji. To właśnie te skutki mogą mieć wysoki priorytet polityczny, co stanowi zagrożenie dla silnej i konsekwentnej polityki naukowo-technicznej.

2. Demografia

Demografia jest kluczowym czynnikiem określającym potencjał rozwoju. Globalna populacja wzrośnie do 2020 r. do poziomu 8,5-9 mld ludzi. Populacja Unii Europejskiej będzie stabilizować się, przy czym region Europy Wschodniej, w tym Polska zagrożony jest nieuchronną depopulacją na skutek negatywnych postaw prokreacyjnych. Warto pamiętać, że Polska już osiągnęła krytyczną zdaniem demografów i ekonomistów proporcję, kiedy jedna osoba pracująca utrzymuje dwie niepracujące (obecnie sytuacja nieco się poprawiła, ale w okresie 2001-2003 zatrudnienie w Polsce wynosiło ok. 13,5 mln przy populacji 38 mln). Zestawienie niekorzystnego trendu demograficznego z trendem globalizacyjnym stawia Polskę w szczególnej sytuacji.

Kraje lepiej od Polski rozwiniętego Zachodu również cierpią na depopulację lub starzenie się społeczeństwa, co oznacza konieczność „uzupełniania" rezerw siły roboczej poprzez kontrolowaną imigrację. Z przyczyn kulturowych, w obszarze UE pracownicy z Polski ze wszystkich obszarów kompetencji (od prostych usług po kadrę naukową) będą pożądanym zasobem, co dodatkowo (mamy tego próbę w chwili obecnej) uszczupli podaż pracy na polskim

rynku.

Co istotne, a na co zwraca uwagę wspomniany James Canton, nasila się już i zacznie się jeszcze bardziej intensyfikować wojna o talenty. Gospodarki krajów rozwiniętych, tracąc wartość dodaną wytwarzaną przez przemysł koncentrować się będą na sektorach wiedzy. Warunkiem ich rozwoju jest jednak dostęp do najcenniejszego i najbardziej chimerycznego zasobu: kapitału ludzkiego. Spodziewać się należy intensyfikacji drenażu mózgów, który dla Polski będzie szczególnie uciążliwy. Jako bowiem kraj biedniejszy nie będziemy w stanie konkurować ofertą pracy w sektorze B+R dla imigrantów, którzy będą wybierać najlepsze centra rozwoju. Już w tej chwili w scenariuszach sektorowych (patrz scenariusz energetyczny) widać wyraźnie, że jedną z głównym barier rozwoju technologii jest starzenie się kadry. Grozi nam, wobec trendów globalnych, że nawet mimo wielkiego wysiłku w kształcenie nowych roczników inżynierów i naukowców, zasilą oni zagraniczne laboratoria oferujące znacznie lepsze uposażenia i szanse rozwoju.

Demografia w połączeniu z czynnikiem żywnościowym oznacza natomiast jeszcze jedną konsekwencję: konieczność powrotu do myśli Thomasa Malthusa.

3. Przesunięcie maltuzjańskie

Musimy pogodzić się, że ilość potrzebnych do rozwoju zasobów ma ograniczony charakter. Od chwili, kiedy w 2005 r. Chiny stały się importerem netto żywności widać, że możliwości produkcyjne żywności w perspektywie 2020 są na wyczerpaniu. Tylko po to, by zaspokoić dodatkowy apetyt Chińczyków na mięso, potrzeba w ciągu najbliższych 10 lat udostępnić 25 mln ha ziemi uprawnej. Niestety, w samych Chinach w tym okresie 4-8 mln ha zostanie utraconych na skutek dewastacji ekologicznej. Jednocześnie wzrost ilości upraw, nawet jeśli znajdzie się potrzebna do tego gleba (o co trudno ze względu na procesy urbanizacji i dewastacji ekologicznej), oznacza wzrost zapotrzebowania na wodę. Rolnictwo jednak już w tej chwili zużywa 70 proc. globalnych zasobów wody pitnej. W konsekwencji rozwój rolnictwa oznacza dalsze uszczuplenie zasobów wody. Już w tej chwili obszarami najbardziej zagrożonymi trwałym brakiem wody są Bliski Wschód (z Izraelem), Indie, Chiny, a więc kraje dysponujące bronią jądrową. Warto pamiętać, że scenariusze lokalnych wojen atomowych są rozważane w strategiach obronnych tych krajów.

Przesunięcie rolnictwa np. do Brazylii, w miejsce wycinanych lasów tropikalnych jest równie problematyczne w świetle badań nad globalnym ociepleniem. O ile bowiem w dorzeczu Amazonki nie zabrakłoby wody i ziemi, to jednak skutkiem rozwoju tego areału może być wzrost globalnego ocieplenia. Ten oznacza dalsze uszczuplenie zasobów wody w obszarach już dotkniętych jej brakiem. Najważniejszą jednak konsekwencją przesunięcia maltuzjańskiego jest wzrost zagrożenia konfliktami, nawet nuklearnymi wywołanymi koniecznością zapewnienia dostępu do podstawowych zasobów.

4. Przesunięcie postpolityczne

Widać wyraźnie wyczerpanie modeli polityki opartej na silnych programach ideologicznych. Po kolei fiasko, jako wzór dla uniwersalnej ścieżki rozwoju odniosły komunizm, neoliberalizm, neokonserwatyzm. Do polityki, w skali państwa i międzynarodowej powraca z jednej strony inspiracja religijna (kraje muzułmańskie), z drugiej realpolityczny pragmatyzm (Chiny, w nieco mniejszym stopniu Unia Europejska). Takie przesunięcie polityczne może oznaczać powrót do polityki równowagi sił, która nieodmiennie prowadziła w historii do militaryzacji, a następnie sięgania po rozwiązania militarne. Pragmatyzm będzie oznaczał m.in. rezygnację z silnego nacisku na promocję idei praw człowieka i demokracji (akceptowanie dyktatur gwarantujących stabilność dostępu do zasobów i kontroli sektora nuklearnego w krajach rozwijających projekty nuklearne).

5. Przesunięcie posthumanistyczne

Związane jest ono z jednej strony z trendami demograficznymi, z drugiej strony z trendami rozwoju technologii i kultury dnia codziennego, zwłaszcza w społeczeństwach krajów najbardziej rozwiniętych. Błyskawiczny rozwój medycyny opartej na zdobyczach biologii molekularnej już spowodował eksplozję popytu na tzw. life-style drugs (prozac, viagra, rhitalin), które już stanowią niemal połowę sprzedaży koncernów farmaceutycznych. Szacuje się, że ponad 25 proc. Amerykanów zażywa prozac. To jednak dopiero początek antropotechnicznego oddziaływania na swoją kondycję. Dalszy rozwój „medycyny spersonalizowanej" oraz nowych terapii opartych na biologii molekularnej, technikach informatycznych i nanotechnologii zapowiada eksplozję popytu na zaawansowane usługi medyczne ingerujące w sposób radykalny w funkcje organizmu. Cyborgizacja na życzenie, jako oferta rynkowa spowoduje dalsze rozwarstwienie społeczne, intensyfikując już dziś opisywane jako bardzo dokuczliwe wykluczenie cyfrowe. Już dziś bowiem zewnętrzny dostęp do technik przetwarzania informacji i komunikacji jest istotnym czynnikiem przewagi konkurencyjnej jednostek i firm na rynku. Co będzie, gdy możliwości wynikające ze stosowania tych technik będą fizycznie uwewnętrznione w naturze człowieka, na skutek modyfikacji cybermedycznych?

Filozofowie z lewej (Habermas) i prawej (Fukuyama) strony ideowego spektrum wskazują, że pojawia się poważne zagrożenie dla podstaw ładu demokratycznego wynikające z radykalnej zmiany koncepcji równości podmiotu, skoro równość ta zostanie w sposób fundamentalny zakwestionowana przez możliwość autokorekty. Dalej zaś pojawiają się kolejne kwestie, jak pokusa nowej eugeniki, sięgającej możliwości genetycznej modyfikacji podmiotu zgodnie z wolą podmiotu zewnętrznego (problem tzw. dzieci na życzenie)[6].

---

6 Joel Garreau, Radykalna ewolucja, przekł. Agnieszka Kloch, Aleksander Michalski, W-wa 2007

Problemy te w istotny sposób dotyczą perspektywy i horyzontu naszych rozważań. Otóż znowu, wobec rozwoju globalizacji „posthumanistyczna" oferta medyczna stanie się dostępna, niezależnie od lokalnego ustawodawstwa także dla obywateli (tych zasobniejszych) Polski. Nie ma także wątpliwości, że wobec trendu starzenia się społeczeństw zachodnich na badania w obszarze antropotechnologii będą przeznaczane coraz większe nakłady. Nakłady te będą w UE czy Japonii wyrazem woli politycznej starzejących się społeczeństw. W kraju takim, jak USA, który nie zrezygnuje w przewidywalnej perspektywie z rozwoju militarnych instrumentów polityki, dodatkowym czynnikiem rozwoju antropotechnologii będą nakłady zbrojeniowe. Wiadomo, że już w tej chwili w ramach tzw. RMA (Revolution in Military Affairs) trwają intensywne prace zarówno nad wyeliminowaniem konieczności użycia „własnej siły żywej" na polu walki, jak i radykalnym poprawieniem parametrów antropologicznych żołnierzy (np. prace nad uzyskaniem przewagi metabolicznej).

Kolejnym aspektem przesunięcia posthumanistycznego jest personalizacja medycyny. Już w tej chwili dostępne są usługi umożliwiające poznanie własnego profilu genetycznego za 1000 USD, w ciągu najdalej 3 lat za tyle samo można będzie poznać sekwencję swojego genomu. Te możliwości otwierają nowy rozdział w medycynie, w którym nowego znaczenia profilaktyka oparta na informacji o osobistych uwarunkowaniach zdrowotnych. Wiadomo, że z możliwości poznania własnego struktury genetycznej skorzystać chce ok. 80 proc. Amerykanów. Jakie będą konsekwencje społeczne, gdy ludzie poznają prawdopodobieństwo zachorowania na Alzheimera i podobne choroby? Jak zmienią się style życia, nawyki kulinarne? Jak trzeba będzie przeorganizować służbę zdrowia, by była w stanie prowadzić zindywidualizowane doradztwo profilaktyczne i psychologiczne? To pytania nie tylko dla amerykańskiej służby zdrowia, ale i dla naszej. Nie można wykluczyć, że w ciągu 5 lat usługa informacyjna w postaci zbadania osobistego profilu genetycznego będzie świadczona przez taką firmę, jak Google za darmo. Mieści się to całkowicie w strategii rozwoju tej firmy, opierającej swą przyszłość na pozyskaniu jak najdokładniejszych profili informacyjnych o swych użytkownikach.

Przesunięcie posthumanistyczne ma także swój wymiar ekstremalny, wyrażający się w ideologii transhumanizmu. Jej prominentnymi przedstawicielami są tacy ludzie, jak Ray Kurzweil, Marvin Minsky, Hans Moravec, Nick Bostrom. Wierzą oni w możliwość uzyskania realnej biologicznej nieśmiertelności w perspektywie 20-30 lat. Nawet jednak w mniej radykalnej perspektywie prognozy wzrostu długości życia mówią, że perspektywa życia nawet 120-130 lat jest zupełnie realną perspektywą dla naszych dzieci i wnuków.

6. Przesunięcie informacyjne I

Kluczowym aspektem gospodarki społeczeństwa informacyjnego jest nie umiejętność przetwarzania informacji, ile władza nad informacją. Analiza sukcesów rynkowych kluczowych przedsiębiorstw epoki informacyjnej: Google,

Amazon, Ebay pokazuje, że ich powodzenia jest skutkiem strategii polegającej na systematycznym kumulowaniu informacji przy współpracy ze swoimi klientami. W efekcie powstaje efekt sprzężenia zwrotnego: im więcej ludzi korzysta z Google, zarówno z wyszukiwarki, jak i usług dodatkowych, tym system Google ma dostęp do większego zasobu danych, które umożliwiają coraz lepiej obsługiwać zarówno klientów indywidualnych, jak i biznesowych, co z kolei zachęca coraz więcej ludzi do korzystania z oferty tej firmy. W rezultacie, w przeciwieństwie do „tradycyjnej" materialnej gospodarki, w świecie Google działa prawo rosnących przychodów: im bardziej firma się rozwija, tym trudniej podjąć z nią realną konkurencję.

Podobna jednak sytuacja ma miejsce w innych obszarach gospodarki. Firmy biotechnologiczne budują swą przewagę konkurencyjną z jednej strony chroniąc swe odkrycia instrumentami własności intelektualnej, z drugiej jednak strony stawiają na tworzenie niepodrabialnych zasobów informacyjnych powstających w efekcie wieloletniej akumulacji danych (np. baza metanomiczna BASF, zawierająca 1,5 mln profili metabolicznych dla 55 tysięcy genów roślinnych).

Zarówno skala tych zasobów informacyjnych, jak i infrastruktura potrzebna do ich utrzymania i rozwoju (system informatyczny Google'a składa się z co najmniej 500 tys. komputerów) oraz instytucjonalne kompetencje intelektualne powodują, że możliwość konkurowania z nimi staje się ograniczona. Powstaje sytuacji monopoli lub quasi-monopoli, która z kolei prowadzi do szybkiego gromadzenia zasobów finansowych (Microsoft ma rezerwy gotówki na poziomie 30 mld dolarów, Apple 15 mld dolarów). Stąd prosta droga od monopolu do monopsonu: Apple w 2006 r. na blisko rok zablokował rynek układów pamięci stałej, rzucając 2 mld dolarów gotówką na zakupu podzespołu kluczowego dla produkcji nowego modelu iPoda. W rezultacie inni producenci, nawet gdyby chcieli, nie mieli szansy podjąć konkurencji w tym okresie w tym segmencie rynku z powodu braku dostaw odpowiednich komponentów.

7. Przesunięcie informacyjne II

Skutkiem rozwoju gospodarki opartej na informacji jest jednak równoległy do monopolizacji i monopsonizacji trend. To rozwój pozarynkowej produkcji społecznej, czyli wszystkich form wytwarzania produktów i usług w logice pozarynkowej, które jednak mają realną wartość użytkową, a więc na rynek wpływają. Konkretne przykłady do środowiska tworzące oprogramowanie typu Linux, Wikipedia, fenomen Web 2.0. Inicjatywy te wyzwalają olbrzymie zasoby innowacyjności wyrażającej się w wielkiej liczbie nierzadko bardzo interesujących inicjatyw kulturowych, inżynierskich, a także naukowych.

Zdaniem Neila Gershenfela[7] z MIT trend ten będzie teraz przesuwał się ze sfery produkcji niematerialnej do produkcji materialnej. Dzięki radykalnej obniżce kosztów narzędzi do szybkiego prototypowania (drukarki 3D, wycinarki laserowe,

7 Neil Gershenfeld, Fab, New York 2005

oprogramowanie projektowe) realne staje się wyposażenie nawet biednych lokalnych wspólnot w minifabryki dysponujące możliwościami precyzyjnej produkcji rzeczy potrzebnych w tejże wspólnocie, a którymi nie jest zainteresowany wielki przemysł (Gershenfeld prowadzi liczne testy polowe tej idei).

Demokratyzacji innowacji działa wieloaspektowo na rynek. Oddziaływanie to ma charakter poprzez zmianę struktury popytu (np. kryzys w przemysłach kultury w chwili, gdy konsumenci kultury zaczęli tworzyć sami dla siebie ofertę; radykalne zmiany w przemyśle oprogramowania). Okazuje się także, że tradycyjne instytucje gospodarcze podejmują wyzwanie nowych form tworzenia innowacji i wdrażają je w swojej praktyce, w ramach modeli takich jak Open Business czy Open Innovation.

Tendencja do demokratyzacji innowacji nie tylko w sferze niematerialnej, ale także materialnej ma potencjalnie istotne znaczenie dla polityki rozwojowej, np. w odniesieniu do polityki energetycznej. W zależności od pewnych strategicznych decyzji ustawia się bowiem brzegowe warunki dla rozwoju całego ekosystemu innowacyjnego. Decyzja o budowie elektrowni atomowej oznacza wybór ścieżki centralizacyjnej, w której rolę głównego koordynatora spada na państwo i duże konglomeraty energetyczne. Podobne pieniądze zainwestowane w promocję innowacyjności społecznej w oparciu o modele Gershenfelda mogą doprowadzić do rozwoju lokalnych inicjatyw polegających na projektowaniu małych źródeł energii, jak i rozwiązań prowadzących do oszczędności, które mogą wielokrotnie zniwelować efekt energetyczny elektrowni. Tyle tylko, że budowa elektrowni jest łatwiej mierzalna niż inicjatywa o charakterze rozproszonym.

Pytanie jednak inne: na ile cenniejsze z punktu widzenia polskiej polityki rozwojowej jest inwestowanie w technologie z importu, w których nigdy nie będziemy w stanie zapewnić sobie autonomicznej pozycji, a na ile stymulowanie innowacyjności społecznej, której skutkiem może być (choć nie musi), rozwój innowacyjnej przedsiębiorczości.

8. Zmiana klimatyczna

Świadomość zmian klimatycznych i radykalne upolitycznienie dyskursu klimatycznego to na pewno jedna z głównych determinant polityki rozwojowej. Warunki brzegowe zostaną określone w ramach Unii Europejskiej i niezależnie od naukowej oceny zmian klimatycznych, a także skuteczności zastosowanych metod przeciwdziałania tym zmianom, będziemy musieli się w swej wewnętrznej polityce dostosować do międzynarodowych zobowiązań.

Z analiz, jakie zaprezentowano podczas Zgromadzenia Ogólnego PAN 13 grudnia 2007 r. wynika, że największy skutek odniosą dwa rodzaje działań. Po pierwsze, oszczędzanie energii i zwiększenie efektywności jej wykorzystania. Po drugie, technologie wychwytu dwutlenku węgla.

To sytuacja otwierająca duże pole dla polskich scenariuszy, daje bowiem

szansę równoległego rozwijania dwóch komplementarnych ścieżek kreowania innowacji. Technologie wychwytu dwutlenku węgla związane są z rozwojem technologii energetycznych (co doskonale pokazują wyniku foresightu energetycznego) i wymagają spójnej, dużej polityki innowacyjnej z udziałem dużych aktorów gospodarczych i naukowych, z udziałem wszak także aktora społecznego, od którego przyzwolenia politycznego zależeć będzie alokacja środków przez polityków.

Z kolei technologie zwiększające efektywność w dużej mierze mogą, a nawet powinny być rozwijane z silnym zaangażowaniem społecznym, polegającym nie tylko na rozwijaniu postaw prooszczędnościowych, ale także innowacyjności technicznej i społecznej. Jednocześnie zaangażowanie także zwiększa zrozumienie dla technologii, oddziałując zwrotnie na klimat sprzyjający rozwojowi „dużych" technologii związanych m.in. z wychwytem węgla.

To tylko jeden z przykładów, ale podobne komplementarne ścieżki rozwoju można wskazać dla innych segmentów. Oprócz wspomnianego już segmentu informatycznego, podobna sytuacja występuje w obszarze rolnictwa i przetwórstwa żywności. Rozwój GMO wymusza uzależnienie od koncernów-właścicieli odmian genetycznych oraz technologii ich uprawy, co z kolei wymusza wzrost kultury rolnej w paradygmacie farmerskim, wielkoskalowym. Na ile można ten model rozwoju równoważyć rozwojem technologii wspierających małe formy gospodarowania i przetwarzania żywności, które sprzyjają także bioróżnorodności i zróżnicowaniu kulturalnemu? Dalej, podobnie rzecz ma się z ochroną zdrowia (równowaga między rozwojem drogich technologii leczenia i profilaktyką w oparciu o najnowsze technologie medycyny spersonalizowanej).

Podsumowanie:

Szkic ten wskazuje tylko kilka elementów kontekstu, jaki powinniśmy uwzględnić tworząc nasze scenariusze. Istotne wydaje się, by wywołać jak najszerszą dyskusję poza gronem ekspertów. W epoce demokratyzacji nie tylko procesów komunikacji, ale także procesów innowacyjnych ograniczenie się do opinii ekspertów może pozbawić nas cennych sygnałów zmian i trendów.

ROZDZIAŁ III

WDROŻENIE SYSTEMU INFORMATYCZNEGO JAKO ZMIANA ORGANIZACYJNA

Dariusz BOGUCKI

1. Zmiana istotą wdrożenia systemu teleinformatycznego

Wdrożenie systemu informatycznego najczęściej definiuje się jako etap cyklu życia systemu, polegający na wprowadzeniu w życie, czyli implementacji projektowanego rozwiązania. Jest to, zatem etap, w którym następuje weryfikacja owoców poprzednich etapów realizacji projektu. A właśnie na tym etapie, statystycznie (jak pokazuje praktyka [4][5][10]) najczęściej pojawiają się problemy projektowe.

Wydaje się, że główna trudność tego etapu wynika ze zderzenia projektu z żywą organizacją, ze swoimi zadaniami, ale też kulturą organizacyjną. Jak to zderzenie może wyglądać, może zilustrować następujący przykład z przed 15 lat, z którego opisem zetknąłem się podczas prac wykonanych w MIPS w zawiązku z projektem ALSO:

W 1993 roku Krajowy Urząd Pracy (KUP) podjął próbę unifikacji oprogramowania wspierającego obsługę bezrobotnych w Rejonowych Urzędach Pracy. Do tego czasu Urzędy same zaopatrywały się w tego typu programowanie – najczęściej u lokalnych twórców / producentów. Nigdy przedtem nie podejmowano prób takiej unifikacji głównie, dlatego że (zgodnie z ówcześnie obowiązującym prawem) takie programy pełniły jedynie rolę pomocniczą w stosunku do rejestracji tradycyjnej. Programy te były niespójne ze sobą, ograniczone funkcjonalnie i technicznie a duża ich liczba (17) powodowała wysokie koszty utrzymania.

KUP zdecydował się rozwiązać problem poprzez centralne zlecenie wykonania programu „zastępczego", który przekazywany by został nieodpłatnie do Urzędów i w perspektywie zastąpił programy używane do tej pory. KUP uważał, że Urzędy (wszak bardzo niezadowolone) z eksploatacji dotychczasowych „pomocniczych" programów, same przestawią się na rozdawany za darmo program COBRA. Był on co istotne nie tylko obiektywnie zdecydowanie lepszy pod względem funkcjonalnym od „konkurentów" ale i dostarczany z pełną dokumentacją użytkownika i administratora, co w ówczesnych czasach było wyjątkiem.

Ta pozornie łatwa akcja zakończyła się kompletnym niepowodzeniem, mimo wykonania oprogramowania na czas i przekazania go do wszystkich jednostek. Żaden z Urzędów Pracy nie przeszedł na nowe oprogramowanie. Analiza, jaką przeprowadzono wskazała następujące przyczyny:

- Potrzeby zgłaszane przez użytkowników w zakresie funkcjonalności systemu były znacznie większe niż to, co oferowały im eksploatowane dotychczas programy jak i program COBRA. Stąd generalne rozczarowanie na zasadzie

„miało być lepiej a jest w sumie tak samo".

- Firma, którą wybrano do dokonania adaptacji programu COBRA nie współpracowała przedtem z Urzędami Pracy. Nie doceniono też siły firm, które dotąd tworzyły oprogramowanie dla urzędów – bardzo szybko stworzyły i wdrożyły w urzędach ulepszone wersje swoich programów.
- Wdrożenie wprowadzono metodą biurokratyczną: z pismem przewodnim rozesłano dyskietki instalacyjne i dokumentację. Nie przeprowadzano szkoleń ani spotkań z użytkownikami a nawet z administratorami. Kontrola wdrożenia odbywała się na podstawie sprawozdań o postępie prac. W KUP nie było osoby, która nadzorowała operacyjnie wdrożenie programu w jednostkach.
- Nie przygotowano programów umożliwiających migrację danych z dotychczasowych baz do nowego programu. Migracja miała się odbywać na zasadzie „ręcznej", co wynikało z błędnego oszacowania zasobu wprowadzonego do baz dotychczasowych programów i ich pomocniczej roli. Z tego też powodu KUP nie przewidział w budżecie środków na opłacenie przenoszenia danych.
- Kierownictwu KUP przedstawiono „propagandowe" terminy wdrożenia, co najmniej dwukrotnie za krótkie jak się okazało. W rezultacie, gdy niektóre z jednostek zaczęły w końcu uruchamiać nowy system, Kierownictwo KUP zniecierpliwione brakiem postępów (oraz perspektywą ówczesnych wyborów) zadecydowało o przerwaniu wdrożenia. Co ciekawe, wszystkie jednostki wróciły do stanu poprzedniego i to w krótkim czasie.

Najciekawszy wniosek zawierała jednak analiza dokonana przez ekspertów Banku Światowego w ramach przygotowania Projektu ALSO – główną przyczyna niepowodzenia było to, że wdrożenie przeprowadzono niezgodnie z regułami zmiany organizacyjnej. Zajmiemy się tym szerzej w dalszej części artykułu.

2. Specyfika zmiany organizacyjnej

Istnieje wiele definicji pojęcia „zmiana organizacyjna". Najtrafniejsza wydaje się podana w [10] zgodnie, z którą **zmiana organizacyjna** jest to zamierzone projektowanie i wdrażanie innowacji strukturalnej, nowej polityki, nowego celu bądź zmiana w filozofii lub stylu działania organizacji. Zmiana organizacyjna zmierza, zatem do przystosowania **całej organizacji** (albo dużej jej części) i tym różni się różni się od rutynowych drobnych zmian, jakie dzieją się, na co dzień w każdej organizacji.

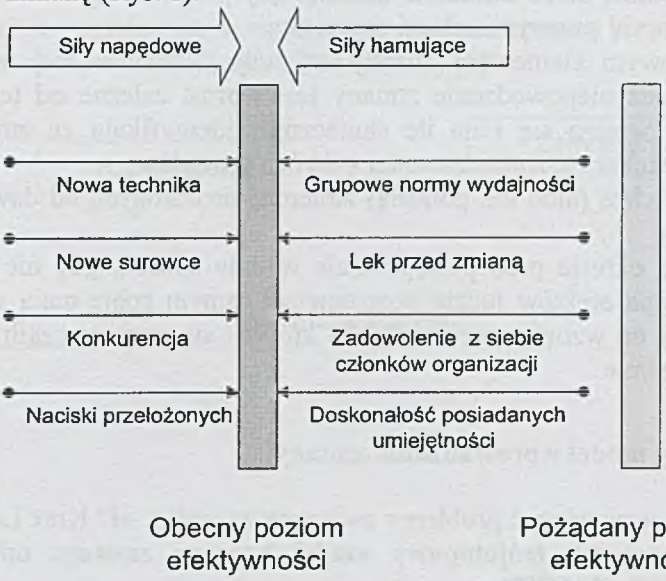
Kluczowym aspektem zmiany organizacyjnej jest to, że zawsze jej „totalny" charakter skutkuje pojawieniem dwóch rodzajów przeciwstawnych dążeń / działań:

- Działania zmierzające do wprowadzenia zmiany i naruszenia istniejącego stanu równowagi organizacyjnej;
- Skierowane przeciwnie dążenia, które przeciwdziałają zmianie mając na celu utrzymanie *status quo*.

Bardzo trafnie zjawisko to opisuje tzw. **model pola sił** zaproponowany w

1951 roku przez Kurta Lewina [6].

Zgodnie z ta teoria, każde zachowanie organizacji jest wynikiem równowagi pomiędzy przeciwstawnie skierowanymi siłami napędowymi i hamującymi zmianę (Rys. 1).



Rys. 1. Schemat pola sił wg. Lewina – Źródło [1]

Przeprowadzenie zmiany (nawet wymuszonej obiektywnymi uwarunkowaniami zewnętrznymi) nie jest, automatyczne. To, że „wszyscy zgadzają się na zmianę" jest pozorne: Model Lewina wskazuje, że jest wiele jawnych i ukrytych źródeł zarówno sił przeciwstawiających się zmianie jak i wiele przyczyn sił napędowych. Lewin podzielił źródła sił hamujących na trzy grupy:

1. **Kultura organizacji**: kształtowanie i utrzymywanie tożsamości organizacji odgrywa chyba największą rolę wśród sił hamujących – służących zachowaniu *status quo*. Pracownicy pozostają w danej organizacji ze względu na to, że pomaga im ona w osiąganiu celów życiowych oraz z tego powodu, że ich postawy, osobowości u przekonania mieszczą się w kulturze organizacji. Dlatego też wielu pracowników identyfikuje się z organizacją i traktuje jej powodzenia i porażki jako sprawę osobistą. W rezultacie mogą się poczuć zagrożeni przez próby wprowadzania radykalnych zmian w kulturze organizacji.

2. **Interes własny**: Pracownicy identyfikując się z organizacją troszczą się zarazem o siebie. W zamian za rzetelnie wykonywana pracę oczekują godziwej zapłaty, zadowalających warunków pracy, pewności zatrudnienia, szacunku i uznania. Kiedy następuje zmiana i pojawia się nieprzyjemny okres dostosowawczy pracownik może go odebrać jako zagrożenie powyższych wartości. Musi upłynąć czas zanim pracownicy dopasują się do nowej struktury.

3. **Poglądy na cele i strategię organizacji**: Misja organizacji i wynikające z niej cele służą zawsze jako ostateczne wytyczne w organizowaniu i koordynacji działalności każdej organizacji. Ta siła skutecznie stabilizuje organizację, zarazem jednak może utrudniać zmianę, gdy pracownicy nie rozumieją i nie identyfikują się z nowymi celami organizacji.

Kluczowym elementem zmiany są, więc ludzie w niej uczestniczący. Powodzenie bądź niepowodzenie zmiany jest wprost zależne od tego, w jakim stopniu ludzie włączą się i na ile skutecznie zidentyfikują ze zmianą. Lewin stwierdził, że większość zmian zawodzi z dwóch powodów:

1. Ludzie nie chcą (albo nie potrafią) zmieniać utrwalonych od dawna postaw i zachowań.
2. Po krótkim okresie prób postępowania w inny sposób, gdy nie przynosi on oczekiwanych efektów ludzie pozostawieni samym sobie mają skłonność do powracania do wzorów zachowań, do których się przyzwyczaili i w których czują się dobrze.

2. Trójetapowy model wprowadzania zmiany

Aby przezwyciężyć problemy związane z „walką sił" Kurt Lewin i Edgar Schein zaproponowali **trójetapowy model procesu zmiany: odmrożenie – zmiana – zamrożenie** [6][7].

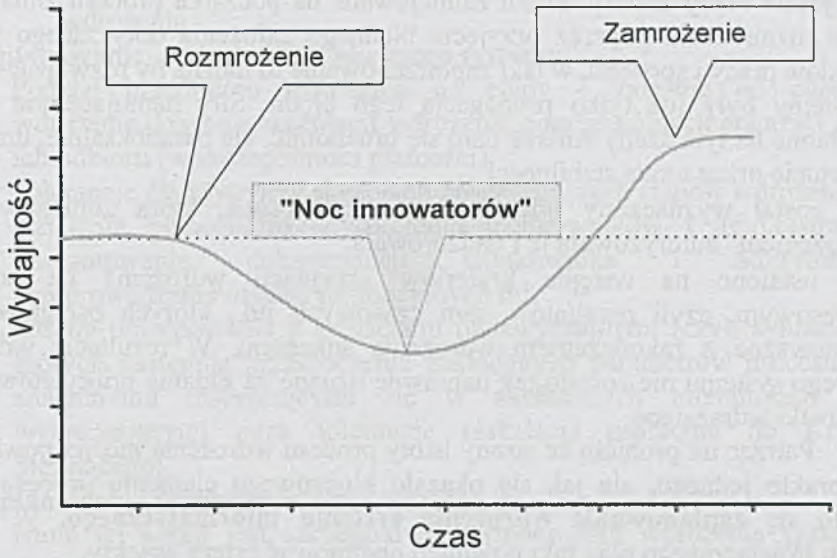
Co ciekawe ów niemłody wszak model jest wciąż aktualny i nader często przywoływany [1][2][3][4] – może dlatego że jest bardzo uniwersalny bo odnosi się zarówno do organizacji jak i zadań przez nią realizowanych (w szczególności projektów gdzie dobrze uzupełnia się z takimi metodykami zarządzania projektami jak PRINCE2®).

Zgodnie z nim można wyróżnić trzy fazy realizacji zmiany w organizacji zgodnej z zachowaniami ludzi:

- **Odmrożenie**: doprowadzenie organizacji do stanu „płynnego" umożliwiającego efektywne wprowadzenie zmian – stwarza rozmach potrzebny do „przeniesienia organizacji na wyższy poziom. W sferze psychologicznej okres ten charakteryzuje się działaniem czynników zaburzających stabilną pozycję ludzi w kierunku określonego nastawienia do zmian czemu towarzyszyć powinno zmniejszanie obaw przed nimi. Zdaniem Lewina i Scheina ta właśnie faza jest **kluczowa** dla właściwego przejścia procesu zmian. W dalszej części pracy przedstawiam przykład potwierdzający tę tezę.
- **Wprowadzenie zmiany**: jest to okres przejściowy, w którym następuje zaszczepienie i wprowadzenie nowych mechanizmów. Jest to zarazem okres niepewności u ludzi spowodowany tym, że borykają się z nowym i niejednoznacznymi, niespotykanymi wcześniej sytuacjami. Ale zarazem świadomość przejściowości tego stanu ten stwarza warunki umożliwiające przeprowadzenie zmiany poprzez szkolenie i praktykowanie ludzi.

- **Zamrożenie**: Ponowne wprowadzenie organizacji „w stan stały", co owocuje integracją zmienionych ról w system powiązań międzyludzkich organizacji. Ludzie zaczynają dostrzegać efekty pozytywne zmian i identyfikować się z nimi.

Model ten zgadza się z empirycznie zaobserwowaną krzywą wydajności pracy organizacji wprowadzającej zmianę (Rys. 2) [6]:



Rys. 2. Krzywa wydajności w procesie zmiany organizacyjnej –źródło [6]

Każda zmiana prowadzi, zatem w pierwszej kolejności do nieuniknionego przejściowego pogorszenia sytuacji, zanim doprowadzi do jej polepszenia (Rys. 2) a odzyskanie poprzedniego poziomu wydajności musi trwać. Płynie stąd szereg ważnych wniosków dla realizacji projektów:

- Ważne jest takie pokierowanie oczekiwaniami zarówno kierownictwa jak i pracowników, by byli przygotowani na czasowy spadek wydajności i to że wyjście z „dołka" zajmie trochę czasu.
- Najczęściej kierownictwo ma mało realistyczne oczekiwania, co do czasu niezbędnego do wprowadzenia zmian. Spadek wydajności i kłopoty, jakie pojawiają się na etapie ich wprowadzania połączony z brakiem jasnej informacji o przyczynach problemów, może wywołać u nich panikę, wycofywanie się i przerwanie zmiany. To zjawisko zwane przez Scheina „**nocą innowatorów**" [66] ma groźne konsekwencje w dłuższej skali czasowej, gdyż zniechęca ludzi do zmian a nawet do uczestniczenia w ich projektowaniu.
- Szczególna rola spoczywa na ludziach, którym powierzono rolę realizatorów zmian. Zmiana oznacza dla nich najczęściej stare obowiązki powiększone o nowe, dodatkowe zadania i stres. Praktyka realizacji projektów informatycznych (a zwłaszcza wdrożeń) obfituje w szczególnie liczne przypadki potwierdzające jak bardzo niezbędne jest zapewnienie im stałego i

skutecznego wsparcia ze strony przełożonych.

4. Zaplanowanie wdrożenia systemu informatycznego

W kontekście modelu trójetapowego nasuwa się następujące spostrzeżenia do przykładu przedstawionego na wstępie:

- Wszystkie błędy zostały, zatem zainicjowane na początku procesu zmiany – w fazie rozmrożenia poprzez przyjęcie błędnego założenia dotyczącego potrzeb urzędów pracy i sposobu, w jaki zapotrzebowanie to można by rozwiązać. Dalsze problemy były już tylko propagacją tego błędu. Siły hamujące nie zostały osłabione na tyle ażeby zmianę dało się uruchomić, ale paradoksalnie, uratowały instytucję przez utratą stabilności.
- Nie został wyznaczony lider zmiany, czyli osoba, która „opiekowała się wdrożeniem" autoryzowała je i nadzorowała.
- Nie ustalono na wstępie kryteriów akceptacji wdrożenia na poziomie biznesowym, czyli rezultatów, ram czasowych itd., których osiągniecie jest równoważne z zakończeniem wdrożenia sukcesem. W rezultacie wdrożenie nowego systemu nie zostało tak naprawdę uznane za zadanie priorytetowe przez jednostki wdrążające.

Patrząc na problem ze strony istoty procesu wdrożenia można powiedzieć, że zabrakło jednego, ale jak się okazało kluczowego elementu procesu, jakim okazało się **zaplanowanie wdrożenia systemu informatycznego.** W świetle modelu trójetapowego plan taki powinien obejmować cztery aspekty:

1. **Aspekt ogólny:** czyli zdefiniowanie ogólnych spraw związanych z wdrożeniem systemu informatycznego, które generalnie nie będą podlegały zmianom w trakcie projektu w szczególności:
   a. **Opis** systemu informatycznego podlegającego wdrożeniu na tle stanu obecnego (inaczej biznesowe uzasadnienie wdrożenia)
   b. Charakterystyka **zakresu wdrożenia** w aspekcie organizacyjnym (gdzie będzie realizowane wdrożenie) i przedmiotowym (wdrażane komponenty sprzętowe, oprogramowanie bądź usługi sieciowe)
   c. **Ogólne kryteria akceptacji wyniku wdrożenia** (na poziomie biznesowym) – równoważne z zakończeniem projektu sukcesem, oraz ogólna tolerancja dla całości wdrożenia (np. możliwe nieprzekraczalne poślizgi czasowe)
   d. **Organizacja wdrożenia**: Podmioty uczestniczące wraz z określeniem ich ról:
      i. Zamawiający (wskazanie osób odpowiedzialnych ze strony Zamawiającego)
      ii. Dostawcy (wskazanie osób odpowiedzialnych ze strony Dostawców)
      iii. Użytkownicy, jeśli są różni od Zamawiającego niezbędne jest określenie zakresu pełnomocnictwa udzielonego Zamawiającemu albo wskazanie ich pełnomocników
   e. Zasady nadzoru nad wdrożeniem, czyli gdzie i w jaki sposób zapada

decyzja o jego uruchomieniu, wstrzymaniu/wznowieniu zatrzymaniu bądź zakończeniu. Innymi słowy wskazanie Komitetu Sterującego tego projektu (o ile zostanie powołany specjalnie do tego celu) bądź wskazanie decydentów komitetu sterującego projektu w ramach, którego realizowane jest wdrożenie;

f. Zasady wewnętrznej komunikacji w projekcie (kto, kogo, o czym, kiedy i w jaki sposób informuje) oraz zasady dokumentowania procesu wdrożenia

2. **Zaplanowanie „rozmrożenia obecnego systemu":**
   a. Podział przedmiotu wdrożenia na etapy – zależnie od charakteru wdrożenia, kryteria akceptacji wdrożenia poszczególnych etapów i zasady ich odbioru (w szczególności płatności).
   b. Tolerancje dla kryteriów akceptacji poszczególnych etapów wdrożenia
   c. Działania pomocnicze – szkolenia użytkowników i administratorów, przygotowanie dokumentacji użytkownika i administratora, przeprowadzenia działań promocyjnych itd.
   d. Zasady postępowania z sytuacjami nadzwyczajnymi (czyli sytuacjami w których następuje przekroczenie zakładanych parametrów procesu) – ze zdarzeniami mieszczącymi się w zakładanych tolerancjach jak i wykraczającymi poza tolerancje (eskalacja problemu do Komitetu Sterującego).
3. **Zaplanowanie przeprowadzenia zmiany:**
   a. Istota tej sekcji jest szczegółowy harmonogram wdrożenia systemu w rozbiciu na poszczególne etapy i lokalizacje (jeśli system wdrażany jest w więcej niż jednej lokalizacji) specyfikujący terminy wdrożenia w układzie data od – data do (a także płatności wynikające z realizacji poszczególnych etapów). Harmonogram ten będzie na bieżąco korygowany w stosunku do harmonogramu bazowego zatwierdzonego wraz z planem i stanowi podstawę do oceny wdrożenia
   b. Druga częścią są scenariusze postępowania z sytuacjami nadzwyczajnymi (np. błędami systemu, jakie ujawniły się w trakcie wdrożenia). Zbiór scenariuszy jest na bieżąco uzupełniany w trakcie zbierania wiedzy o rozwiązywanych sytuacjach nadzwyczajnych (w trakcie wdrożenia)
4. **Zaplanowanie „zamrożenia / ustabilizowania systemu":**
   Generalnie jest to opis przejścia z fazy wdrożenia do fazy utrzymania systemu i odpowiedzialności po stronie dostawców, zamawiającego i użytkowników. Zwłaszcza usuwanie błędów jakie ujawniły się w trakcie i po wdrożeniu systemu – czyli wnioski z wykazu scenariuszy postępowania z sytuacjami nadzwyczajnymi.

Literatura

1. *„Zarządzanie projektami IT"*, Joseph Philips,", Onepress, Gliwice, 2005;
2. *„Walka postu z karnawałem"*, Tomasz Byzia, cykl artykułów,

«Computerworld» Nr 37 – 47 / 2002;
3. *„Sprzedawcy srebrnych kul”*, Tomasz Byzia, cykl artykułów, «Computerworld» Nr 38/2002 – 03 / 2004;
4. *„Pusty portfel projektów”*, Tomasz Byzia, Zarządzanie funkcjami IT nr specjalny «Computerworld» 2005;
5. *„10 przyczyn porażki”*, Antoni Bielewicz, , «Computerworld» Nr 8/2007;
6. Liz Clarke, *„Zarządzanie zmianą” z serii «Podstawy Zarządzania»*, Gebethner i Spółka Warszawa, 1997;
7. Włodzimierz Serwiński cykl artykułów *„10 przykazań w zarządzaniu projektami informatycznymi”*, «Computerworld» Nr 19 – 29 / 1999;
8. Strategor, *„Zarządzanie firmą – Strategie, Struktury, Decyzje, Tożsamość”*, PWE Warszawa, 1999;
9. James A. Stoner, Edward R. Freeman, Daniel R. Gilbert *„Kierowanie”*, PWE Warszawa, 1999;
10. Andrzej Polak „Wdrażanie systemu informacyjnego – model idealny”„ CEO grudzień 2002

ROZDZIAŁ IV

STRATEGICZNE CELE E-NAUCZANIA

Wiesław BYRSKI

Motto

Quisquid agis prudente agas et respice finem
(Cokolwiek czynisz, rób dobrze i końca patrzaj)

Wprowadzenie

Nowe technologie można opisywać i analizować z różnych punktów widzenia. Można je doskonalić i doprowadzać do perfekcji technicznej. Warto jednak zadać sobie pytanie, jaki jest cel tej technologii, jakie zadanie spełnia - nie ona jako taka, tylko jako środek do celu. Zatem warto zastanowić się, zanim zaczniemy masowo stosować nowe technologie jaki cel z ich użyciem realizujemy? Czy dotychczasowa przyczyna wprowadzania tej właśnie technologii jest dalej aktualna? A może zmiany, jakie zostały wywołane przez właśnie tę technologię spowodowały, jako uboczny skutek, że zniknął, albo silnie zmodyfikował się sam cel? Łatwo znaleźć analogie historyczne, że takie zjawisko zachodzi, czego ukoronowaniem może być odkrycie McLuhana z dziedziny komunikacji społecznej, że „medium is a message".

Czy sam fakt, że coś można zrobić jest wystarczającym uzasadnieniem wprowadzania nowej technologii? Znowu –z licznych przykładów – widać, że tego rodzaju zmiany celu zasadniczego można było antycypować, a przynajmniej post factum wyjaśniać w dziedzinie nauk społecznych. Najczęściej twórcy technologii nie są w stanie objąć wyobraźnią nadchodzące przemiany. Słynna jest wypowiedź szefa IBM z lat pięćdziesiątych XX w, że najwyżej 5 komputerów zaspokoi potrzeby całego świata, która wynikała z ówczesnej interpretacji zastosowania nowej technologii obliczeń. Sensem i celem istnienia komputerów było, jak się wydawało wtedy, rozwiązywanie problemów matematycznych. Tego, że nastąpi taka zdecydowana zmiana strategicznego celu stosowania komputerów (chyba) nikt nie przewidywał. Na pewno nie wiedział tego producent komputerów. Jednak, jak wiemy z historii, nie wpłynęło to negatywnie na rozwój informatyki, ani na losy IBM.

Drugiej wielkiej pomyłki IBM zapewne żałuje do dziś. Dzisiejszy standard mikrokomputerów to wynalazek IBM z lat osiemdziesiątych. Ale IBM potraktował PC jako mało użyteczną zabawkę, szacując roczny rynek zbytu na kilkanaście tysięcy sztuk. Strategicznym celem IBM był rynek „prawdziwych" komputerów. Konsekwencją było oddanie rynku mikrokomputerów IBMPC światu poprzez niepobieranie licencji na ich konstrukcję, a praw do systemu operacyjnego DOS

małej firmie Microsoft. Już po dekadzie nastąpiła zmiana strategicznego znaczenia komputera osobistego, ze znanymi konsekwencjami.

Zatem można sądzić, że twórcy technologii rzadko mają właściwą wyobraźnię, dla przewidzenia skutków jej użycia. Czy zatem forsując stosowanie nowej technologii w nauczaniu nie wpadamy w jakąś pułapkę?

W tym artykule autor próbuje dokonać dyskusji problemów związanych z określaniem celów strategicznych nauczania gdy zacznie się używać nowej e-technologii, co, jak na razie, robi się nieudolnie, z miernymi wynikami i przy braku przekonujących wzorców. A więc jakie są strategiczne cele nauczania?

1. Dobrze postawione cele

Po co istnieją koty? Aby łapać myszy. Tak postawiony cel dla na pierwszy rzut oka wygląda logicznie. Rozszerzmy nieco cel strategiczny istnienia kota – kot ma wyłapać myszy. Ale jak wyjaśnić istnienie myszy? Żeby koty miały co łapać? Widać w tym momencie, że cel dla kota był źle postawiony.

Niektórzy pamiętają informatyzację szkół za pomocą Elwro-Juniorów. Oczywiście cel strategiczny był, jak się wydawało sensowny, jak jednak okazało się dość szybko ówczesna technologia nie nadawała się do realizacji tak określonego strategicznego celu. Tego rodzaju pomyłki przy stawianiu celów strategicznych dla nowych technologii zdarzają się ciągle. Gdy pojawiły się komputery w dydaktyce wyznaczony dla nich cel strategiczny był oczywisty i jak się wydawało ze wszech miar słuszny: komputer miał pomagać w dydaktyce stwarzając dla nauki zupełnie nowe horyzonty. Gdy obecnie prowadzi się zajęcia ze studentami w pracowni komputerowej sporo wysiłku kosztuje przymuszenie uczniów do działań, które realizowałyby postawiony cel strategiczny i odrywanie uczniów od innych według nich ważniejszych zastosowań komputera (poczta, gadu-gadu, gry komputerowe, obrazki, następne zajęcia itp.).

Przypomnijmy sobie dyskusję na przykład dyskusję o strategicznym znaczeniu informatyzacji firm wywołaną przez N. Carra. Car dowodził, że przypisywanie strategicznego znaczenia informatyce przestało być prawdziwe i informatyka nie daje już przewagi konkurencyjnej firmom, które ją zastosowały. Według Cara informatyka w organizacji stała się niezbędną infrastrukturą, która, wprawdzie konieczna, ale nie gwarantuje uzyskania przewagi strategicznej. Czyli już po dekadzie rozwoju zmienił się cel strategiczny tej technologii.

2. Ewolucja postawionych celów

Gdy powstawało radio, jego misją była nauka, oświata, wiedza, kultura i rozrywka. Takie same cele zakładała telewizja. Internet narodził się na Uczelniach, jego cel strategiczny był oczywiste – łatwiejszy dostęp do wiedzy. W relatywnie krótkim czasie strategiczne cele radia, telewizji i internetu uległy zmianie i tamtejsze cele są tylko niewielką częścią realizowanych obecnie. Głównym celem tych mediów stała się rozrywka i komercja. Medium is a message - to kwintesencja

ewolucji powyższych celów

3. Fałszywie postawione cele

Gorzej, gdy od samego początku cele nie są uczciwie sformułowane i pozornie realizowany jest cel wskazywany, a właściwy jest zupełnie inny. Słynne jest historia 70 lat zatruwania środowiska ołowiem, pod pretekstem lepszego wykorzystania paliwa silnikowego. W latach 20 XXw. duPont wynalazł dodatek do benzyny czteroetylek ołowiu, który poprawiał jej właściwości. Równocześnie General Motors wynalazł silniki samochodowe, które potrafiły efektywnie wykorzystać ten dodatek i w efekcie bijąc konkurencję silników samochodowych Forda. Zmowa tych dwóch koncernów doprowadziła do wyemitowania do atmosfery miliardów ton ołowiu w ciągu 70 lat, mimo ostrzeżeń o wysokiej szkodliwości tego pierwiastka. Umiejętna i wyrafinowana akcja np. czteroetylek ołowiu nazwano nie – jakby wskazywała na to chemiczna nazwa „ołowiną" tylko niewinnie „etyliną" sprowadzała się do pokazania zupełnie innego niż prawdziwy cel strategiczny. Nawet w czasie II wojny światowej samoloty niemieckie latały na benzynie z dodatkiem ołowiu na licencji duPonta.

Drugi przykład manipulowania celami strategicznymi jest współczesny. Po rozpowszechnieniu się telefonów komórkowych pojawił się problem niebezpieczeństwa związanego z używaniem ich w czasie prowadzenia samochodu. Celem strategicznym ruchu drogowego jest bezpieczeństwo, zatem naturalne wydaje się wprowadzenie konieczności posiadania zestawów głośnomówiących. Tylko czy one załatwiają problem? Przecież po takim rozwiązaniu okazuje się, że niebezpieczne jest trzymanie telefonu w ręce, podczas gdy zdrowy rozsądek sugeruje, że niebezpieczeństwo sprowadza odwracanie uwagi poprzez sam fakt rozmowy z kimś, kto nie śledzi razem z nami drogi oraz manipulacje na klawiszach w czasie nawiązywania połączenia.

Te dwa przypadkowe przykłady pokazują, że nie sposób oddzielić technologii od biznesu. Co więcej, pokazują że zalety technologii w ogólnym rozrachunku nie muszą przynosić wartości dodanej, jak również pokazują, że możnaby bez trudu ustalić czy właściwie postawiono cele strategiczne sugerowanej nowej technologii. Zadajmy sobie zatem pytanie jakie są strategiczne cele e-learningu?

4. Rozum kontra ewolucja

Spróbujmy wcześniej przeanalizować realne możliwości rozwiązania problemu ustalania właściwych celów a priori. W szczególności zastanowimy się czy technologia rozwija się świadomie, pod kontrolą rozumu, czy też rządzą jej rozwojem ślepe prawa ewolucji

Na poziomie operacyjnym, czyli konkretnej potrzeby, rozum wykazuje swoją przydatność. W pewnym momencie historii Edison stworzył słynną fabrykę wynalazków. Sam wynalazek jest często kwestią przypadku, ale jego praktyczne

wykorzystanie wymaga długotrwałej, żmudnej pracy. Doskonałe efekty przyspieszające rozwój dają również wszelkie konkursy i zawody. Szczególnie wyraźnie widać ten efekt w informatyce, wystarczy wspomnieć maszynę tabulującą Holleritza – efekt konkursu rządu USA, programy grające w szachy czy najnowszy challange pojazdów samosterujących na pustymi Mohave i kolejny w mieście.

Ale dalszy los wynalazku kierowany jest poprzez siły ewolucji, a rozum nie ma wiele - jeśli w ogóle - do powiedzenia:

- porażająca historia 70 lat ołowiny
- DDT
- globalna zmiana klimatu
- nawet ewidentne analogie nie wstrzymują przed popełnianiem tych samych błędów. A może analogie - jak proroctwa - widać i można zrozumieć dopiero *post factum?*
- nie byłoby nic złego w funkcjonowaniu ewolucji jako siły sprawczej postępu. Ale ewolucja działa jak francuski bricouler:
- buduje z resztek, z tego, co pod ręką
- z odpadów
- znajdując zupełnie inne zastosowanie tego, co jest
- rozlicznych przykładów w przyrodzie znajdziemy wiele:
- płuca powstały z pęcherza pławnego
- nogi - z płetw
- mówimy, jemy, oddychamy tym samym otworem
- analogicznie działa ewolucja w technice:
- samochód - karoca z obciętym dyszlem
- urządzenia wejścia/wyjścia – dalekopis,
- nośniki programów – dalekopisowa taśma dziurkowana, potem karty dziurkowane z maszyn tabulujących, a wcześniej z krosien Jacquarda,
- pamięci zewnętrzne - magnetofony
- telewizja poprzez fale radiowe, a telefon przez kabel

Monitor ekranowy jako podstawowe i masowe urządzenie wyjściowe pojawił się późno, mimo, że prototypy przecież istniały. Dopiero po latach pojawiły się potrzeby wskazujące na konieczność inwestowania w technologię monitorów ekranowych. Stało się tak dopiero wtedy, gdy pojawiły się nowe cele jakie spełniać miało we-wy. Przedtem nie istniały, pojawiły w miarę ewolucji technologii przetwarzania danych z przetwarzania wsadowego na przetwarzanie on line. A więc gdy pojawił się nowy cel strategiczny otrzymywania wyników: „do obejrzenia", dotychczasowym celem było „trwałe zapisanie wyników, gdyż ich ponowne otrzymanie zajmuje za dużo czasu oraz nie m gdzie przechować".

Czy dałoby się dojrzeć tę zmianę strategii wykorzystywania komputerów wcześniej? W tym celu należy przyjrzeć się celom strategicznym spełnianym w obecnej technologii, a następnie dokonać próby ewolucji tych celów w nowym środowisku i nowej technologii. Warto pamiętać, że należy analizować prawdziwe, a nie pozorne cele, w innym przypadku nie ma szans na choćby minimum trafności

przewidywań.

5. Ważkie - strategiczne? - cele nauczania

W Historii niebieskiego mundurka opisany jest konflikt jaki pojawił się między zwolennikami gęsiego pióra a nowym wynalazkiem piórem stalowym. Przyczyną konfliktu było naruszanie przez stalówkę strategicznego celu nauki pisania - właściwego charakteru pisma. Gdy gęsie pióra przegrały rywalizację, kilkadziesiąt lat później wdały się w konflikt z wiecznym piórem, które też, podobno, psuło charakter pisma. Kilkanaście lat później, kolejny konflikt wywołało pojawienie się długopisu.

Teraz takich konfliktów już nie ma, gdyż charakter pisma stał się nieistotnym czynnikiem w nauczaniu pisania. Stało się tak z powodu powszechnego używania innego sposobu zapisu, ręczne pisanie jest, albo będzie wkrótce, pewnym kultywowanym reliktem. Po przeczytaniu tych słów nie bardzo można zrozumieć, dlaczego szkoła (podstawowa-liceum) nie pozwala używać komputera w nauce pisania. Komputer wprawdzie jest obecny w procesie dydaktycznym, ale w charakterze mechanicznej, pozbawionej wszelkich udogodnień merytorycznych pomocy. Zapewne celem strategicznym nauki pisania jest umiejętność ... I znowu jest konflikt.

Wojsko zawsze przygotowuje się do wojny, która już była. Szkoły uczą tego, co istnieje. Czy nie jest niepokojące, że uczymy studentów udając, że komputery nie istnieją? Nie mówię o komputerze jako źródle wiedzy, ale o komputerze, który uczy. Np. czy są w szerszym użyciu programy egzaminujące wiedzę, a nie fakty (typowe testy)? Czy niechęć studentów do nauczenia się czegokolwiek tak, aby zapamiętać w bardziej trwały sposób, nie jest dalekowzrocznym przeczuciem, że nie trzeba się uczyć na pamięć, bo wszystko już niedługo będzie łatwo dostępne? Z chwilą stworzenia wreszcie wygodnego interfejsu (słuchawka w uchu, wyświetlacz na siatkówce oka, klawiatura w zębach, bezprzewodowa łączność z inteligentnymi bazami wiedzy) oraz dojrzałej komunikacji człowiek-maszyna wtedy nastąpi rewolucja nie tylko nauczania.

6. Strategiczne cele e-nauczania

Od dawna istniały podręczniki programowane, które stosowały technikę podziału treści na małe fragmenty, testowanie opanowania materiału poprzez pytania kontrolne po tych fragmentach oraz odpowiednie sterowanie procesem samouczenia na podstawie odpowiedzi na pytania kontrolne. Cel i realizacja były jasne - dlaczego zatem nie odniosły sukcesu edukacyjnego?

Potem - równolegle - funkcjonowało nauczanie korespondencyjne - czym się różni od e-nauczania? Podobnych pytań można zadać wiele:

- Czym różni się wideo-konferencja od audio-konferencji?
- Czym różni się wykład on-line od wykładu zarejestrowanego?
- Czy e-lerning uniknie katastrofalnego spadku jakości, jakie było udziałem

nauczania korespondencyjnego?

To, czego dostarcza nowa technologia nauczania typu e-learning to niskie koszty dla właściciela, wygoda dla użytkownika i zysk dla dostarczycieli. Ale są to w rzeczywistości cele biznesowe, trudno w tej chwili wyartykułować edukacyjne cele zorientowane na technologię zdalnego e-nauczania i komputery. Trochę sytuacja przypomina stosowanie elektronicznego bata, hamulców z ABS i nawigacji satelitarnej dla transportu z użyciem wozów konnych. Dostarcza się użytkownikowi porcji materiału dobranego i przygotowanego dla starej, tradycyjnej technologii nauczania. Co więcej, korzystając z nowoczesnej technologii równocześnie ignorowany jest fakt, że zdobywaną wiedzę będzie się wykorzystywało właśnie w tym nowoczesnym środowisku. Widoczny jest wyraźny rozdźwięk miedzy możliwościami i zastosowaniem. Próbuje się eksplorować e-technologię na oślep i bez wyartykułowanych celów, z nadzieją, że same się znajdą. Brakuje ewidentnie nowych dydaktycznych celów strategicznych dla nowego e-środowiska.

Wnioski

Wywód ten nie sugeruje, że e-nauczanie jest błędną ścieżką, ciekawostką technologiczną bez wartości dydaktycznej. Oznacza jedynie, że zadania, jakie nakłada się na e-lerning są niewłaściwe i niedopasowane do już istniejących możliwości oraz wyraźnie widocznych przyszłych kierunków rozwoju. Niektóre realizowane zadania są wyraźną pomyłką, a nawet nadużyciem. Na podstawie kilku podanych analogii można sądzić, że właściwe cele pojawią się na drodze prób i błędów w procesie ewolucyjnego poszukiwania. Wtedy wszyscy będą twierdzić, że tak właśnie miało być od początku. Autor sądzi, że można by przyspieszyć poszukiwania.

Literatura

1. Applehans W., Globe A., Laugero G.: Managing Knowledge, A Practical Web-Based Approach, Addison-Wesley, 1999
2. Byrski W. , Systemy informacyjne z bazą wiedzy, PRET, 2002
3. Byrski W., Informatyczne wspomaganie procesu tworzenia strategii organizacji, w: Informatyka w gospodarce globalnej. Problemy i metody, red. J. Kisielnicki i inni WNT, Warszawa-Szczyrk 2004
4. Byrski W., Zarządzanie strategiczne organizacją w czasach burzliwych, w: Informatyka w gospodarce globalnej. Problemy i metody, red. J. Kisielnicki i inni WNT, Warszawa-Szczyrk 2003
5. Byrski W., Cele strategiczne przekazywania wiedzy w środowisku nowych technologii informatycznych w: Zeszyt Naukowy nr. 6 Wyższa Szkoła Zarządzania i Bankowości, Kraków 2007
6. Cellary W., Porównanie uniwersytetu dziś i jutro w: Cellary W. (red)

Polska w drodze do globalnego społeczeństwa informacyjnego. Raport o rozwoju społecznym. Warszawa, UNDP, 2002
7. Demarest M., Long Range Planning 30, 1997, issue 3
8. Haber L., Akademicka społeczność informacyjna. Na przykładzie środowiska akademickiego Akademii Górniczo-Hutniczej, Uniwersytetu Jagiellońskiego i Akademii Ekonomicznej, Kraków, AGH 2005
9. Hartmann J.C.M, Why is it so difficult to combine experience and theory in business decisions? Hydrocarbon Processing, November 2002
10. Kubiak M., Wirtualna edukacja, Warszawa, MICOM 2000
11. Obłój K., Strategia organizacji, PWE, 2002

ROZDZIAŁ V

WYMIAROWANIE W PRAKTYCE INŻYNIERII OPROGRAMOWANIA

Beata CZARNACKA-CHROBOT

1. Wprowadzenie

Informatyczne przedsięwzięcia konstrukcyjne oraz wdrożeniowe wymagające kastomizacji w przeważającej większości przypadków nie spełniają tradycyjnych kryteriów skuteczności ich realizacji. Zgodnie z rezultatami prowadzonych systematycznie od połowy lat 90-tych kompleksowych analiz instytucji badawczej Standish Group, współczynnik sukcesu dla tego typu projektów nigdy nie przekroczył 35% (por. [JOHN05], [STAN07]). Oznacza to, że znaczna większość takich przedsięwzięć albo kończy się niepowodzeniem całkowitym: według najnowszych badań projekty porzucone stanowią 19% podejmowanych przedsięwzięć (por. [STAN07]), albo przekracza zaplanowane koszty i/lub czas realizacji, dodatkowo charakteryzując się zwykle niską zgodnością z wymaganiami wyspecyfikowanymi przez użytkownika: aktualne badania wskazują na 46% projektów zakończonych niepowodzeniem częściowym (por. [STAN07]). W związku z tym Standish Group szacuje, iż straty wynikające z zainwestowania środków w takie przedsięwzięcia, bez uwzględnienia strat z powodu utraconych przez użytkownika możliwości biznesowych, wynoszą w zależności od roku od 22 do 55% wydatków przeznaczonych na realizację informatycznych przedsięwzięć konstrukcyjnych i wdrożeniowych z kastomizacją (por. [STAN03]).

Niska skuteczność realizacji przedsięwzięć zmierzających do rozwoju systemów oprogramowania użytkowego to jedna z zasadniczych przyczyn, dla których w inżynierii oprogramowania podjęto próby wykorzystania doświadczeń płynących z innych dyscyplin o charakterze inżynierskim. Wszak jak stwierdził z pewną celową przesadą Alfred Spector: *„Mosty są zwykle budowane w zaplanowanym czasie, w ramach zaplanowanych kosztów i się nie zawalają. Systemy oprogramowania zaś nigdy nie są oddawane na czas, ani w granicach budżetu. Dodatkowo - zawsze się zawalają"* (por. [STAN95]). Toteż, mimo znaczących różnic w specyfice produktu i procesu, pojawiło się przekonanie, że realizacja oprogramowania byłaby skuteczniejsza, jeżeli obiekty te podlegałyby wymiarowaniu - podobnie jak w innych dziedzinach inżynierskich, dla których stanowi ono cechę immanentną.

Przyjmując zatem w inżynierii oprogramowania znany postulat Galileusza: *„Licz to, co policzalne, mierz to, co mierzalne, a to, co niemierzalne, uczyń mierzalnym"* (por. [KOPA78]), problematyce wymiarowania produktów programowych i procesów ich wytwarzania poświęcono liczne publikacje, które ujmują tę tematykę w różnych kontekstach. Postulaty dotyczące wymiarowania

doczekały się również stworzenia wielu standardów lub modyfikacji pod tym kątem standardów istniejących, zwłaszcza w ostatnim czasie, co świadczy o rosnącej potrzebie zwiększenia skuteczności realizacji takich przedsięwzięć dzięki możliwości podejmowania racjonalnych, bazujących na obiektywnych pomiarach decyzji inwestycyjnych.

Niewiele jest jednak badań empirycznych, które umożliwiałyby sformułowanie wiążących konkluzji odnośnie obecnego podejścia do wymiarowania w praktyce inżynierii oprogramowania, jak również co do wykorzystywanych w tym celu metod, mierzonych atrybutów, a jeszcze mniej takich, które pozwoliłyby na wiążące stwierdzenie o zmianie postawy wśród praktyków wobec problematyki wymiarowania. Aktualne badania wskazują z jednej strony na dostrzeganie konieczności wymiarowania, szczególnie na poziomie zarządzania, z drugiej jednak na potrzebę podejmowania w dalszym ciągu działań mających na celu przekonanie praktyków o istniejących w tym zakresie możliwościach. Niniejszy artykuł ma na celu zaprezentowanie rezultatów takich badań na tle różnych podejść do wymiarowania w inżynierii oprogramowania.

2. Podejścia do wymiarowania w inżynierii oprogramowania

Podejścia do wymiarowania atrybutów procesów i produktów programowych można podzielić w oparciu o propozycję K. Richinsa (por. [RICH01, s. 3.259-3.260]) na trzy następujące kategorie:

1. Modele i metody, w ramach których wyznaczane są kierunki postępowania w celu prawidłowego przebiegu wymiarowania oprogramowania i procesu jego wytwarzania. Ich przykłady to m.in.:
   - ✓ model oceny i doskonalenia procesów programowych CMMI (ang. *Capability Maturity Model Integration*)[1];
   - ✓ metodyka PSM (ang. *Practical Software and Systems Measurement*)[2];
   - ✓ metoda GQM (ang. *Goal, Question, Metric* – Cel, Pytanie, Analiza)[3];
   - ✓ Goal-Driven Software Measurement Method[4];
   - ✓ PSP (ang. *Personal Software Process*)[5];
   - ✓ TSP (ang. *Team Software Process*)[6];
   - ✓ Six-Sigma[7];
   - ✓ ITIL (ang. *Information Technology Infrastructure Library*)[8];

[1] Por. [CMMI06].
[2] Por. np. [GANT01, s. 3.108-3.125], [PRAC00].
[3] Por. np. [FENT00, s. 107-109].
[4] Por. np. [PARK96].
[5] Por. np. [HUMP96].
[6] Por. np. [HUMP99].
[7] Por. np. [CAVA03].
[8] Por. [ITIL07].

- ✓ Balanced Scorecard[9];
- ✓ SPC (ang. *Statistical Process Control*)[10].

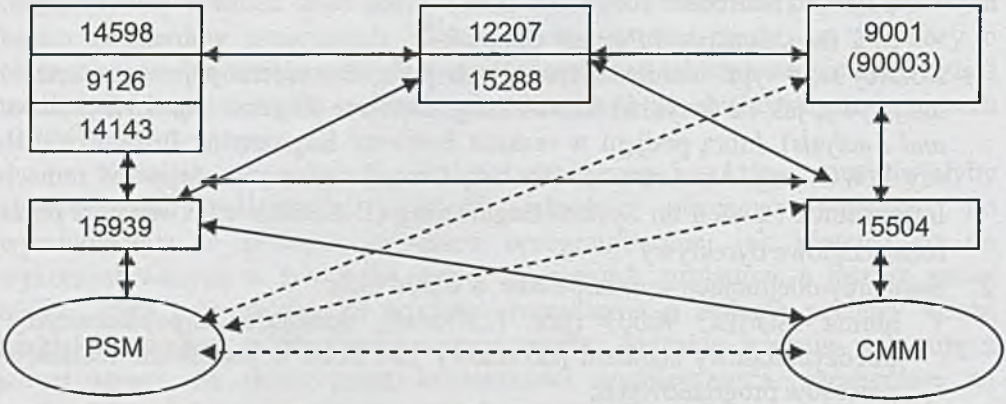
Rozwój tego typu ustrukturalizowanych podejść wspierany jest przez takie inicjatywy, jak na przykład SEMA (ang. *Software Engineering Measurement and Analysis*), którą podjęto w ramach Software Engineering Institute (SEI), czy MWG (ang. *Measurement Working Group*) - grupę działającą w ramach International Council on System Engineering (INCOSE)[11], jak również przez różne rządowe dyrektywy[12].

2. Standardy obejmujące wymiarowanie, a wśród nich:
   - ✓ norma ISO/IEC 90003 (por. [ISO04a]), opisująca najpopularniejszy międzynarodowy standard jakościowy ISO 9001 w kontekście realizacji procesów programowych;
   - ✓ norma ISO/IEC 15504, zwana SPICE (por. ISO98]), dotycząca oceny procesu programowego;
   - ✓ norma ISO/IEC 12207 (por. [ISO95]), definiująca procesy dotyczące wytwarzania produktu programowego, które powinno się poddawać ocenie zgodnie z modelami przeznaczonymi dla poszczególnych procesów (np. SPICE, tzw. reprezentacja ciągła CMMI);
   - ✓ standard ISO/IEC 14598 (por. [ISO01]), w którym unormowano proces przeprowadzania oceny produktu programowego[13].
3. Standardy poświęcone wymiarowaniu, w tym:
   - ✓ norma ISO/IEC 15939 (por. [ISO07a]), wyznaczająca ogólne standardy dla procesu wymiarowania w zgodzie z norma ISO/IEC 15288 (por. [ISO02a]), która definiuje procesy cyklu życia systemu;
   - ✓ standard ISO/IEC 9126 (por. [ISO01-04]), opisujący powszechnie obowiązujący model jakości oprogramowania, jedyny obejmujący metryki służące ocenie poszczególnych jej atrybutów (por. [KOBY05, s. 85]);
   - ✓ norma ISO/IEC 14143 (por. [ISO98-07]), dotycząca wymiarowania rozmiaru funkcjonalnego produktów programowych.

Powiązania pomiędzy najważniejszymi z wyżej wymienionych podejść do wymiarowania przedstawiono na rys. 1.

---

[9] Por. np. [KAPL07].
[10] Por. np. [OAKL07].
[11] Por. np. [BOEH03].
[12] Najbardziej znana z nich to *Department of Defence (DoD) Directive 5000.2-R*, obejmująca procedury obowiązujące dla zakupów na rzecz Departamentu Obrony Stanów Zjednoczonych w ramach programów typu MDAP (ang. *Major Defense Acquisition Programs*) i MAIS-AP (ang. *Major Automated Information System Acquisition Programs*) – por. [DOD96].
[13] Opis jest zróżnicowany ze względu na osobę dokonującą oceny (projektanci, nabywcy i tzw. ewaluatorzy).



Rys. 1. Powiązania między kluczowymi podejściami do wymiarowania w inżynierii oprogramowania Źródło: [RICH01, s. 3.260].

Część z wymienionych podejść jest zatem ukierunkowana *explicite* na wymiarowanie (np. metodyka PSM, norma ISO/IEC 15939), inne zaś traktują ów proces jako jedną z zalecanych kategorii działań (np. model CMMI, norma ISO/IEC 15504). Co więcej, niektóre z nich są ukierunkowane na ocenę produktów, inne zaś na ocenę procesów. Do tych pierwszych zaliczają się metody i standardy w sposób ogólny normujące proces przeprowadzania oceny produktu (np. norma ISO/IEC 14598) oraz podejścia służące wymiarowaniu poszczególnych jego atrybutów, w tym na szczególną uwagę zasługuje norma ISO/IEC 9126 służąca ocenie atrybutów jakościowych produktu programowego oraz norma ISO/IEC 14143 dedykowana do oceny jego tzw. rozmiaru funkcjonalnego (por. [CZAR04]).

Normę ISO/IEC 14143 w pierwszej wersji ogłoszono pod koniec lat 90. ubiegłego wieku, jednak jej intensywny rozwój miał miejsce w ostatnich latach, kiedy to także zrewidowano pierwszą część omawianego standardu (por. [ISO07b]). Wszystkie jego części, podobnie jak normy ISO/IEC dotyczące poszczególnych metod wymiarowania rozmiaru funkcjonalnego, są zgodne ze standardem ISO/IEC 15939, zaktualizowanym w 2007 r. i wyznaczającym ogólne zasady dla procesu wymiarowania zgodnie z normą ISO/IEC 15288, w której definiuje się procesy cyklu życia systemu. Wśród metod wymiarowania funkcjonalnego ISO i IEC jak dotąd uznały tylko cztery z ok. 20 istniejących w postaci następujących norm:

- ✓ ISO/IEC 20926 (por. [ISO03a]) - opisuje metodę punktów funkcyjnych w wersji IFPUG (ang. International Function Point Users Group);
- ✓ ISO/IEC 20968 (por. [ISO02b]) - obejmuje metodę punktów funkcyjnych w wersji Mk II;
- ✓ ISO/IEC 24570 (por. [ISO05]) - dotyczy metody punktów funkcyjnych w wersji NESMA (ang. Netherlands Software Metrics Association);
- ✓ ISO/IEC 19761 (por.[ISO03d]) - opisuje metodę pełnych punktów funkcyjnych w wersji COSMIC (ang. Common Software Measurement

International Consortium).

Istnieje wiele modeli jakości produktów programowych (por. [KOBY05, s. 71-89]), jednak tylko w normie ISO/IEC 9126 zaproponowano zbiór metryk, za pomocą których można ocenić poszczególne atrybuty ich jakości (funkcjonalność, użyteczność, niezawodność, wydajność, łatwość konserwacji, przenośność)[14]. W standardzie tym proponuje się ocenę jakości oprogramowania przy wykorzystaniu metryk zewnętrznych (por. [ISO03b]), wewnętrznych (por. [ISO03c]) oraz metryk jakości użytkowej (por. [ISO04b]). Te ostatnie wykorzystywane są tylko w rzeczywistym środowisku działania systemu, jako że służą do pomiaru stopnia faktycznego zaspokojenia wymagań określonych użytkowników przez dostarczony produkt – uwzględnia się przy tym osiąganie przez końcowych użytkowników celów odnoszących się do skuteczności, produktywności, bezpieczeństwa i satysfakcji związanej z wykorzystaniem produktu w określonym rzeczywistym kontekście jego użycia (por. [ISO03b, s. 12]). Metryki zewnętrzne z kolei służą do pomiaru jakości produktu poprzez ocenę jego zachowania się w trakcie wykonywania w środowisku, którego jest on częścią[15] – mogą być zatem stosowane jedynie podczas testowania i eksploatacji ocenianego produktu (por. [ISO03b, s. 12-13]). Metryki wewnętrzne natomiast można wykorzystywać już na wcześniejszych etapach projektowania, kiedy produkt nie jest jeszcze wykonywalnym programem – umożliwiają one więc pomiar jakości rezultatów pośrednich, dzięki czemu pozwalają przewidzieć jakość produktu końcowego, dostrzec ewentualne problemy i podjąć w reakcji na nie odpowiednie działania, a w rezultacie tę jakość ocenić (por. [ISO03b, s. 12-13]).

Wykorzystanie metryk jakości produktu zdefiniowanych w normie ISO/IEC 9126 przedstawia się następująco (por. [ISO03b, s. 12, 14]):

- ✓ po wyspecyfikowaniu wymagań jakościowych należy określić priorytetowe atrybuty jakości produktu końcowego - zazwyczaj wraz z podcharakterystykami;
- ✓ następnie powinno się wyznaczyć właściwe metryki zewnętrzne wraz z dopuszczalnym zakresem ich wartości, a zatem przedstawić wymagania wobec jakości produktu w formie kryteriów ilościowych;
- ✓ kolejno definiuje się odpowiednie metryki wewnętrzne i ich dopuszczalny zakres, tak aby można było osiągnąć wymagany poziom metryk zewnętrznych i wykorzystać je do pomiaru jakości produktów pośrednich;
- ✓ ocena jakości produktu z perspektywy użytkownika w rzeczywistym środowisku jego funkcjonowania następuje przy wykorzystaniu metryk jakości użytkowej i zależy od danego użytkownika końcowego, przy czym mierzone są nie tyle własności samego oprogramowania, co raczej rezultaty jego działania.

Omawiana norma zakłada, że jakość produktu programowego jest

[14] Przy czym ocena ta ma charakter pośredni, jako że mierzy się w rzeczywistości cechy bardziej szczegółowe, tj. tzw. podcharakterystyki (por. np. [ISO03b, s. 19-24]).

[15] Obejmującym inne elementy systemu informatycznego, np. sprzęt komputerowy, inne oprogramowanie lub systemy, użytkowników (por. [KISI05, s. 25-26]).

uwarunkowana jakością procesu jego wytwarzania[16]. Przyjmując taki punkt widzenia należy stwierdzić, że poprawa jakości produktu wymaga udoskonalenia jakości procesu (por. [KOBY06, s. 115]). Dlatego powinno się oceniać nie tylko jakość produktu, ale również jakość procesu wytwarzania oprogramowania, co dodatkowo może pomóc wykazać prawdopodobne zależności między nimi.

Procesy realizacji produktu programowego można oceniać na poziomie określonego przedsięwzięcia, jak i na poziomie organizacji wytwarzającej oprogramowanie. Do oceny i poprawy jakości procesu stosuje się modele jego oceny i doskonalenia, do których zalicza się m.in. (por. np. [FENT00, s. 88, 109-112], [KOBY05, s. 125-135]): dwie odmiany modelu CMMI - tzw. reprezentację etapową CMMI (ang. *CMMI Staged Representations* – CMMI-SR) oraz tzw. reprezentację ciągłą CMMI (ang. *CMMI Continuous Representations* – CMMI-CR), SPICE, jak również standard ISO/IEC 90003[17].

Niektóre z tych modeli (np. CMMI-SR) wykorzystuje się w celu oceny poziomu dojrzałości organizacji poprzez przydzielenie jej do jednego z jej pięciu poziomów (od 1. do 5. - im poziom wyższy, tym organizacja bardziej dojrzała), zaś za pomocą innych (np. CMMI-CR, SPICE) można oceniać każdy realizowany w firmie proces dotyczący wytwarzania produktu programowego poprzez zakwalifikowanie go na jeden z sześciu poziomów możliwości (od 0. do 5.) - przy czym procesy te są zdefiniowane w normie ISO/IEC 12207. O ile pierwszy rodzaj modeli ma za zadanie raczej wspomóc zleceniodawców w wyborze właściwego zleceniobiorcy, dzięki czemu firmy zajmujące się wytwarzaniem oprogramowania dążą do uzyskania jak najwyższego poziomu dojrzałości, o tyle ocena dokonywana przy wykorzystaniu drugiej ich grupy ma charakter bardziej wewnętrzny (przynajmniej pierwotnie), pozwalający pracownikom na uzyskanie informacji o procesach wymagających udoskonalenia (por. [KOBY06, s. 112]).

W modelach oceny i doskonalenia procesu programowego przywiązuje się dużą wagę do wymiarowania (por. [FENT00, s. 110-111]. Modele oceny każdego ze szczegółowych procesów realizowanych w organizacji (np. CMMI-CR) wyróżniają procesy pomiarowe jako jeden z procesów głównych, natomiast modele oceny dojrzałości organizacji (np. CMMI-SR) wymagają, aby organizacja znajdująca się na określonym jej poziomie realizowała bieżące pomiary produktów i procesów, w tym m.in. mierzyła produktywności pracy, oraz gromadziła dane niezbędne do dalszych analiz, a przede wszystkim do estymacji atrybutów przyszłych przedsięwzięć (por. [KOBY06, s. 113]). Dla modelu CMMI-SR w obecnej jego wersji procesy wymiarowania wymagane są już od drugiego poziomu dojrzałości (por. [CMMI06, s. 36-38]).

Wymiarowanie atrybutów przedsięwzięć informatycznych (np. pracochłonności, czasu, kosztów) i ich produktów (np. zakresu funkcjonalnego,

---

[16] Założenie to wydaje się logicznie uzasadnione, jednak nie istnieją badania, które w pełni dowodziłyby, iż poprawa procesów programowych determinuje wyższą ogólną jakość produktów programowych (por. [FENT00, s. 111], [KOBY05, s. 25]).

[17] Istnieją również inne tego typu modele, np. model Bootstrap i Trillium, jednak już rzadko wykorzystywane.

jakości) wymaga podjęcia działań o dużym zróżnicowaniu merytorycznym, zastosowania niejednokrotnie bardzo odmiennych podejść, toteż bywa często postrzegane w praktyce jako trudne, praco- i czasochłonne. Jednak wymiarowanie stanowi kluczowy środek do doskonalenia tych obiektów i z tego powodu właśnie *„nadszedł czas, aby rozwój oprogramowania i systemów skierować na stosowanie wymiarowania w stopniu (...) podobnym do innych dyscyplin inżynierskich, gdzie wykorzystuje się je od wielu dekad"* (por. [GOLD03, s. 22-23]).

3. Wymiarowanie w praktyce inżynierii oprogramowania – rezultaty badań Software Engineering Institute

Jak się wydaje najbardziej aktualną, kompleksową, rozległą i spójną próbę odpowiedzi na pytanie o podejście do wymiarowania w praktyce inżynierii oprogramowania podjął w 2006 r. Software Engineering Institute (SEI) w ramach programu *Software Engineering Measurement and Analysis* (SEMA). Celem tej inicjatywy jest rozpowszechnianie wiedzy na temat wszelkich aspektów związanych z wymiarowaniem w inżynierii oprogramowania, tak aby organizacje zaangażowane w jego rozwój, jak również ich klienci pozyskali możliwość skutecznego i efektywnego zarządzania podejmowanymi przedsięwzięciami dzięki wykorzystaniu stosownych modeli, metod i technik. Efekty podjętego przez SEI badania zawiera obszerny raport (por. [KASU06]), który jednak nie pokazuje jeszcze trendów w praktycznym podejściu do wymiarowania, a jedynie stan obecny, jako że stanowi wynik dopiero pierwszego z serii zamierzonych corocznych analiz[18].

Grupa analityków działająca w ramach inicjatywy SEMA postawiła przed omawianymi badaniami następujące cele (por. [KASU06, s. 1]):

1) Scharakteryzowanie stopnia, w jakim praktycy wytwarzania oprogramowania stosują wymiarowanie w swojej pracy oraz postrzeganej przez nich wartości tego procesu;
2) Scharakteryzowanie podejść wykorzystywanych w praktyce do wskazania sposobu definiowania i użycia miar oraz najpopularniejszych rodzajów miar stosowanych przez praktyków wytwarzania oprogramowania;
3) W przyszłości: wskazanie trendów w powyższych obszarach badawczych.

W odniesieniu do pierwszego z wymienionych celów rezultaty przeprowadzonego badania wskazują, iż (por. [KASU06, s. 6-17]):

- Ponad 60% pracowników zaangażowanych w wytwarzanie oprogramowania zarówno dostarcza informacje bazujące na wymiarowaniu, jak i je wykorzystuje. Wśród samych użytkowników takich informacji przeważają

[18] Badanie przeprowadzono na próbie prawie 2 tys. praktyków w obszarze inżynierii oprogramowania (pracujących dla organizacji wytwarzającej oprogramowanie lub wspomagających pracę takiej jednostki), przy czym wszyscy oni kontaktowali się z SEI w latach 2004-2005, znają więc prawdopodobnie produkty i usługi oferowane przez ten instytut.

osoby odpowiedzialne za zarządzanie. W prawie 70% przypadków cel wymiarowania, tj. gromadzenia danych lub ich raportowania, jest zwykle zrozumiały, jednak pomiędzy poszczególnymi grupami zawodowymi występują istotne różnice: o ile ok. 65-75% menadżerów zazwyczaj ów cel uznaje za oczywisty, o tyle tak twierdzi tylko ok. 50% programistów. Ów cel jest również bardziej zrozumiały w przedsiębiorstwach aniżeli w instytucjach rządowych.

- W niemal 95% przypadków wymiarowanie jest wykorzystywane do zrozumienia jakości produktów lub usług, nad którymi się pracuje, przy czym w 45% przypadków często, w 39% okazjonalnie, zaś w 11% rzadko. Tymczasem jedynie 36% pracowników zaangażowanych w wytwarzanie oprogramowania uważa, że definicje miar stosowane w ich organizacjach są zrozumiałe i logiczne. Dalsze 32% zgadza się z tym stwierdzeniem, ale nie w pełni. O ile miary są zrozumiałe i logiczne dla ok. 70-75% menedżerów, o tyle za takie uważa je jedynie ok. 60% programistów i analityków.
- Więcej niż 90% praktyków zaangażowanych w wytwarzanie oprogramowania uważa, że wymiarowanie nieco pomaga (10%), pomaga (35%) lub znacznie pomaga (45%) w efektywniejszym funkcjonowaniu zespołów w zestawieniu z sytuacją, kiedy nie jest ono realizowane. I znów znaczne różnice występują pomiędzy różnymi grupami zawodowymi: ok. 95% zarządzających zgadza się, że wymiarowanie jest w tym celu przydatne, podczas gdy teza ta znajduje potwierdzenie wśród niespełna 85% programistów.
- Ponad 45% zespołów projektowych często stosuje udokumentowane procesy gromadzenia danych niezbędnych do wymiarowania, 30% robi to okazjonalnie, natomiast 15% rzadko. Osoby odpowiedzialne za zarządzanie wykorzystują je znacznie częściej niż programiści (ok. 80% *versus* ok. 60%). Podobne rzecz się ma w przypadku stosowania udokumentowanych procesów sprawozdawczych odnośnie danych stanowiących rezultat wymiarowania.
- Tylko w ok. 43% przypadków często wykorzystuje się wymierne kryteria w stosunku do wytwarzanych produktów lub dostarczanych usług, w prawie 53% przypadków są one stosowane okazjonalnie (38%), rzadko (13%) lub nigdy (niemal 2%). Przy czym kryteria te dostrzega 85% zarządzających, a jedynie ok. 65% programistów.
- W sytuacji, gdy przekraczane są zaplanowane wielkości atrybutów przedsięwzięcia działania korygujące są często podejmowane tylko w 40% przypadków, zaś w 35% okazjonalnie. W 14% takich sytuacji podejmuje się je rzadko, a w 5% w ogóle. I znów występują znaczne różnice w spojrzeniu na ów problem w zależności od grupy zawodowej: ok. 80% menedżerów twierdzi, że działania korygujące podejmowane są często lub okazjonalnie, zaś w przypadku programistów twierdzi tak jedynie 60%. Jednak nawet w sytuacji, gdy istnieją wymierne kryteria dla wytwarzanych produktów lub dostarczanych usług, działania korygujące nie zawsze są podejmowane.

Za zasadnicze wnioski płynące z analizy tego obszaru badawczego autorzy raportu uznali następujące (por. [KASU06, s. 29-32]):

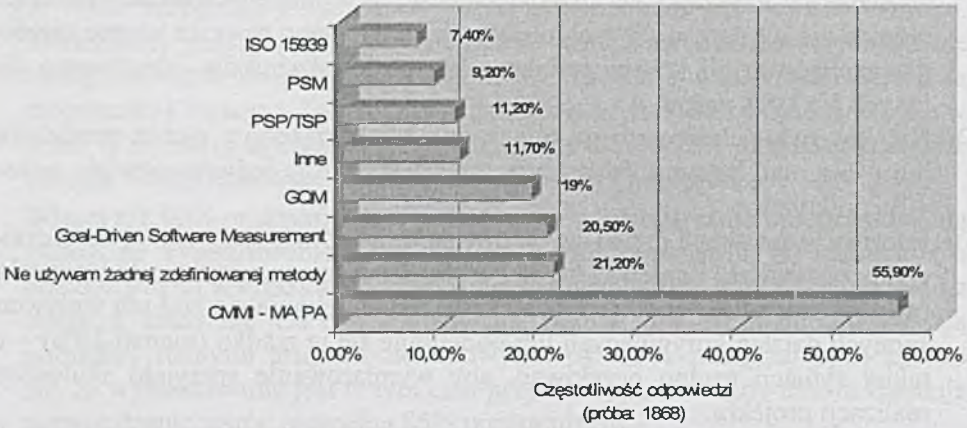
1) Wraz ze wzrostem rozmiaru organizacji rośnie stopień zaangażowania w proces wymiarowania;
2) Menedżerowie i pozostały personel (programiści, analitycy, inżynierowie) postrzegają proces wymiarowania z innej perspektywy: ci pierwsi dostrzegają w nim większą wartość;
3) Istotne różnice w podejściu do wymiarowania pomiędzy instytucjami rządowymi a firmami dotyczą jedynie postrzegania wartości procesu wymiarowania z perspektywy efektywniejszego funkcjonowania zespołów oraz zrozumienia definicji miar (w obu przypadkach większe wartości wskaźników uzyskano dla przedsiębiorstw) – w innych kwestiach znaczące różnice nie występują. W tych obszarach zanotowano również istotne różnice dla analizowanych krajów (większe wartości wskaźników odnotowano dla innych niż USA państw);
4) Nie jest zadowalające stosowanie wymiernych kryteriów wobec produktów lub usług, nad którymi się pracuje: często stosuje je jedynie niewiele ponad 40% praktyków;
5) Informacje uzyskane dzięki wymiarowaniu niejednokrotnie nie są skutecznie wykorzystywane, ponieważ w razie przekroczenia planowanych atrybutów przedsięwzięcia zdecydowanie za często nie podejmuje się pod ich wpływem żadnych działań korygujących lub podejmuje się je rzadko (niemal 20%) – w takiej sytuacji trudno oczekiwać, aby wymiarowanie sprzyjało skutecznej realizacji projektu.

W odniesieniu do drugiego z postawionych celów rezultaty badania przeprowadzonego przez SEI wykazały, że (por. [KASU06, s. 17-24, 27-28, 32-33]):

- Do interpretacji sposobu definiowania i używania miar wykorzystuje się (por. rys. 2):
  - ✓ najczęściej, bo w 56% przypadków, model CMMI, a mówiąc dokładniej jego obszar procesu wymiarowania i analizy (ang. *Measurement and Analysis Process Area – MA PA*)[19], przy czym w niemal 30% przypadków jest to jedyny stosowany w tym celu model;
  - ✓ rzadziej, bo w ok. 20% przypadków, Goal-Driven Software Measurement Method, podobnie jak metodę GQM (ang. *Goal, Question, Metric* – Cel, Pytanie, Analiza), jednak bardzo rzadko są one używane jako jedyne rozwiązania (odpowiednio: 5% i 3%), a zwykle towarzyszy im model CMMI;
  - ✓ w ok. 12% przypadków metody PSP/TSP (ang. *Personal Software Process/Team Software Process*), w nieco mniejszej ich liczbie (ponad 9%) metodykę PSM (ang. *Practical Software and Systems Measurement*) - ich samodzielne użycie jest również znikome;
  - ✓ jedynie w ok. 7,5% przypadków normę ISO/IEC 15939;

[19] Por. [CMMI06, s. 178-197], [GOLD03, s. 20-24]. Wypracowanie obszaru wymiarowania i analizy obywało się w ścisłej współpracy ze specjalistami z Practical Software and Systems Measurement Support Center, ISO i IFPUG.

- ✓ w prawie 12% przypadków inne rozwiązania (np. metody wypracowane przez własne organizacje);
- ✓ w ponad 21% przypadków nie wykorzystuje się w omawianym celu żadnych zdefiniowanych metod wymiarowania (drugie miejsce pod względem częstotliwości odpowiedzi po CMMI)[20];
- ✓ w większości przypadków, bo w niemal 60%, stosuje się równolegle kilka metod (stąd przedstawione na rys. 2 udziały nie sumują się do 100%), przy czym najpopularniejsze są kombinacje zawierające model CMMI[21].



Rys. 2. Metody wymiarowania wykorzystywane w inżynierii oprogramowania według rezultatów badań SIĘ Źródło: [KASU06, s. 18].

- W obszarze badania dotyczącym najczęściej wykorzystywanych w praktyce miar przez takie miary rozumiano te, które zazwyczaj objęte są sprawozdawczością, założono również ograniczony ich zbiór. Znalazły się w nim wskaźniki: postępu w harmonogramie prac (97% odpowiedzi), nakładów pracy przydzielonych zadaniom (93%), zidentyfikowanych ryzyk (90,4%), zidentyfikowanych błędów (90%), błędów usuniętych (86%), stabilności wymagań (74%) i przyrostu kodu (63%). Dodatkowo poproszono praktyków o wskazanie pozostałych, nie nazwanych w badaniu miar – uzyskano szerokie spektrum odpowiedzi, z których najbardziej interesujące dotyczą stosowania: wskaźników finansowych (9%), produktywności (3,6%), miar powiązanych z klientem (ang. *customer-releted measure* - 2,9%), z kodem programu (ang.

[20] Co więcej, w odpowiedziach „Inne" (por. rys. 2) znajdziemy kolejne 2% takich odpowiedzi.

[21] Autorzy badania zastrzegają jednak, że duża popularność modelu CMMI, a więc rozwiązania proponowanego przez SEI może wynikać z faktu dobrania do badania specjalistów znających przypuszczalnie produkty i usługi oferowane przez ten instytut, co należy mieć na uwadze przy interpretacji rezultatów badania odnośnie podejść wykorzystywanych w praktyce do wskazania sposobu definiowania i stosowania miar.

code-releted measure - 2,0%), z zasobami/personelem (2,0%), wskaźnika wartości wypracowanej (ang. *earned value* - 1,5%) oraz pomiaru rozmiaru produktu (1,3%).

4. Uwagi końcowe

Analiza rezultatów powyżej zaprezentowanego badania SEI upoważnia, zdaniem autorki, do następujących dodatkowych wniosków:

- Wyniki badania dają raczej odpowiedź na pytanie o najczęściej wymiarowane w celach sprawozdawczych atrybuty poszczególnych obiektów (tj. *co* jest przedmiotem wymiarowania), aniżeli na pytanie o najpopularniejsze w praktyce rodzaje miar (czyli *jak* się wymiaruje poszczególne atrybuty, np. rozmiar produktu, jego niezawodność, produktywność pracy etc., które można mierzyć w różnych jednostkach za pomocą różnorodnych metod). Niemniej jednak badanie wykazuje, że najczęściej obejmuje się sprawozdawczością czas i pracochłonność realizacji przedsięwzięcia, a zatem wymiarowane są w pierwszym rzędzie atrybuty procesu programowego (postęp prac w czasie, nakłady pracy, również ryzyka), a dopiero później produktu programowego (zidentyfikowane i usunięte błędy, czyli jego niezawodność, przyrost kodu, a zatem długość programu).
- Dobór z góry założonych w badaniu atrybutów może wprawdzie nastręczać pewne wątpliwości, jednak w efekcie prośby o wskazanie innych nie uzyskano precyzyjnych odpowiedzi, jako że sporo z nich pokrywa się z przyjętym ich zbiorem (np. śledzenie czasu: 19%, aspekty jakościowe/dotyczące błędów: 14%, powiązane z harmonogramem: 6%, z procesem: 5%, z wymaganiami: 3%, z ryzykiem: 2%, a 17% wskazało odpowiedź „Inne")[22]. Toteż można z dużą dozą prawdopodobieństwa przypuszczać, że bez określonego zestawu atrybutów rezultaty byłyby jeszcze mniej precyzyjne.
- O ile osoby odpowiedzialne za zarządzanie organizacją wytwarzającą oprogramowanie faktycznie dostrzegają wartość informacji dostępnych dzięki wymiarowaniu i uznają cel tego procesu za oczywisty, w związku z czym często stosują dlań udokumentowane procesy, jak również znajdują w nim środek pomocny w efektywniejszym funkcjonowaniu zespołów, o tyle badanie nie wskazuje, że pierwszorzędne znaczenie mają te miary, które dotyczą atrybutów zewnętrznych: czas i pracochłonność, jak również długość programu to wszak atrybuty wewnętrzne (dwa pierwsze - procesu, ostatni – produktu). Z kolei tak wydawałoby się istotne dla zarządzających atrybuty zewnętrzne, jak np. koszt procesu, jego opłacalność czy produktywność pracy, są mierzone niezwykle rzadko (wskaźniki finansowe: 9%, produktywność: 3,6%, miary powiązane z zasobami/personelem: 2,0%, wskaźnik wartości wypracowanej: 1,5%).

[22] Por. [KASU06, s. 28].

- Zastanawiający jest minimalny stopień wykorzystania miar powiązanych z klientem (2,9%), jak również fakt, że pomiar aspektów jakościowych, kluczowych dla użytkownika, ograniczony jest praktycznie jedynie do niezawodności produktu (błędy zidentyfikowane i usunięte)[23]. Co więcej, w badaniu wykazano, że praktycy widzą w wymiarowaniu środek pomocny w zrozumieniu jakości produktów lub usług, jednak środek ów nierzadko zawodzi ze względu na niezrozumiałe i nielogiczne definicje miar.
- Niewątpliwie zjawiskiem niepokojącym jest częste stosowanie wymiernych kryteriów w odniesieniu do produktów lub usług jedynie przez mniej niż połowę praktyków, chociaż kryteria te są znane, bo nie stosuje ich nigdy tylko 2% specjalistów. W tym obszarze zastanawia również fakt, że z jednej strony miara długości kodu programu (przyrost kodu) znalazła się wśród stosunkowo popularnych miar[24], a z drugiej strony wskaźniki odnoszące się do kodu programu (ang. *code-releted measure*) są jednak rzadko stosowane, co potwierdzałoby słuszność sentencji jednego z bardziej znanych praktyków zajmujących się wytwarzaniem oprogramowania, W. Gatesa, który uważa, że: *„Pomiar postępów w programowaniu za pomocą linii kodu jest jak pomiar postępu w budowie samolotu za pomocą jego ciężaru."*[25]
- Tymczasem na pomiar rozmiaru produktu - prawdopodobnie w jednostkach innych niż linie kodu[26] - wskazuje jedynie 1,3% odpowiedzi. W związku z tym nasuwa się hipoteza, iż kluczowe według badania atrybuty, tj. pracochłonność i czas realizacji przedsięwzięcia, są wyprowadzane na bazie rozmiaru produktu mierzonego za pomocą linii kodu bądź w ogóle bez uwzględniania tego atrybutu. Wobec powyższego nie dziwi fakt, iż planowany w ten sposób czas i koszty są często i w dużej skali przekraczane.
- Dodatkowo z badania wynika, że produktywność mierzy się jedynie w 3,6% przypadków, co oznacza, że przy szacowaniu pracochłonności, stanowiącej podstawę dla estymacji czasu i kosztów realizacji przedsięwzięcia, nie uwzględnia się zazwyczaj tego atrybutu, a ma on istotny wpływ na trafność ocen szacunkowych i w rezultacie na ocenę skuteczności realizacji przedsięwzięcia.

Wobec powyższego trudno nie zgodzić się z wnioskiem końcowym płynącym z omawianego badania: *„Z perspektywy inicjatywy SEMA podjętej w ramach SEI w praktyce wymiarowania ciągle występuje znaczna luka pomiędzy bieżącym stanem rzeczywistym a stanem pożądanym. (...) Rezultaty badania*

---

[23] W badaniu wskazuje się także na dodatkowy wynik (14%) dla pomiaru aspektów jakościowych, jednak równie dobrze mogą one dotyczyć jedynie właśnie błędów (ang. *defects/quality issues*).

[24] Przyrost kodu był składnikiem z góry założonej w badaniu grupy elementów podlegających wymiarowaniu.

[25] *„Measuring programming progress by lines of code is like measuring aircraft building progress by weight."* (por. http://en.wikiquote.org/wiki/Bill_Gates, 18.08.2007).

[26] Te jednostki bowiem były uwzględnione w innych odpowiedziach.

prowadzą do wniosku, że ciągle dużo trzeba zrobić, aby organizacje skutecznie stosowały wymiarowanie w celu doskonalenia swoich procesów, produktów i usług" (por. [KASU06, s. 29]).

Natomiast wynikająca z badania opinia o stosunkowo dużej popularności w praktyce inżynierii oprogramowania modelu CMMI, mimo opatrzenia jej zastrzeżeniem o dobraniu do badania praktyków znających przypuszczalnie rozwiązania SEI, nie jest odosobniona. Według W. Melo, w USA CMMI stanowi *„bezspornie najpopularniejszy model"* (por. [MELO06, s. 5]), w odniesieniu zaś do Europy badania German Association for Information Technology, Telecommunication and New Media (BITKOM) z 2004 r. wskazują, że według ponad 70% organizacji ten model w przyszłości będzie odgrywał wiodącą rolę wśród modeli cyklu życia systemu (por. [1, s. 15]). N. Fenton ocenia, że już model CMM (wersja źródłowa dla modelu CMMI) *„na całym świecie szybko został uznany za wzorzec do usprawniania procesu programowania"* (por. [FENT00, s. 88]), podobnie sądzi również M. Flasiński, uważając go za *„najbardziej popularną metodę zapewnienia jakości procesu odpowiadającego przeprowadzeniu przedsięwzięcia informatycznego"* (por. [FLA06, s. 171]). Zdaniem A. Kobylińskiego z kolei z dużą dozą prawdopodobieństwa można założyć, iż model CMMI będzie nadal rozwijany, co wynika głównie z następujących faktów: silnego wsparcia finansowego ze strony rządu USA (Departamentu Obrony), zgodności modelu z wieloma powszechnie zaakceptowanymi normami (np. ISO/IEC 15504), rzetelnego gromadzenia uwag mających na celu jego udoskonalenie przez autorów modelu, a przede wszystkim z jego wykazanej przez lata użytkowania przydatności (por. [KOBY05, s. 219]). Co więcej, na drugim miejscu pod względem częstotliwości odpowiedzi (ponad 20%) znalazła się grupa praktyków deklarująca, iż nie wykorzystuje żadnych zdefiniowanych metod pomocnych w wymiarowaniu, a inne normy, w tym ISO (poza ISO/IEC 15939) i IEEE (ang. Institute of Electrical and Electronic Engineers), i takie metody, jak Six-Sigma, ITIL, Balanced Scorecard czy SPC, wskazano w znikomej liczbie odpowiedzi (każdą po mniej niż 1% ogółu badanych)[27]. Dlatego logiczną konsekwencją przedstawionych w niniejszym opracowaniu rozważań będzie przybliżenie podejścia do wymiarowania w obecnej wersji modelu CMMI.

Literatura

1. R. Baltus, *Ergebnisse einer BITKOM Befragung zu System Life Cycle Modellen*, BITKOM, Bonn, November 2004.
2. B.W. Boehm, J.E. Rieff, G.D. Thomas, R. Valerdi, *COSYSMO – Constructive Systems Engineering Cost Model*, International Council on System Engineering, 2003 Symposium, Crystal City, VA, June 30, 2003.
3. R.R. Cavanagh, R.P. Neuman, P.S. Pande, *Six Sigma. Sposób poprawy*

[27] Por. [KASU06, s. 18-19].

wyników nie tylko dla firm takich, jak GE czy Motorola, K.E. Liber, Warszawa 2003.
4. CMMI Product Team, *CMMI for Development, Version 1.2*, Software Engineering Institute, Carnegie Mellon University, Pittsburg, August 2006.
5. B. Czarnacka-Chrobot, *Pomiar rozmiaru funkcjonalnego systemu informatycznego - sposób na "chaos permanens"?*, w: *Współczesne kierunki rozwoju informatyki*, praca zbiorowa pod red. P. W. Fuglewicza, B. Jackowskiego, E. Mizerskiej, A. Ostaszewskiej, Materiały XX Jesiennych Spotkań PTI, Polskie Towarzystwo Informatyczne, Katowice-Mrągowo, listopad 2004, s. 111-120.
6. *DoD Directive 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*, Department of Defense, March 15, 1996.
7. N.E. Fenton, *Zapewnienie jakości i metryki oprogramowania*, w: *Inżynieria oprogramowania w projekcie informatycznym*, Wyd. II rozsz., red. J. Górski, Mikom, Warszawa 2000.
8. Flasiński M., *Zarządzanie projektami informatycznymi*, Wydawnictwo Naukowe PWN, Warszawa 2006.
9. D. Gantzer, G. Roedler, *Practical Software and Systems Measurement*, Proceedings of a Seminar On Metrics, International Council on System Engineering (INCOSE), Hampton, Virginia, October 23-24, 2001.
10. D. Goldenson, J. Jarzombek, T. Rout, *Measurement and Analysis in Capability Maturity Model Integration Models and Software Process Improvement*, *CrossTalk*, July 2003.
11. W.S. Humphrey, *Introduction to the Personal Software Process*, Addison-Wesley Professional, December 1996.
12. W.S. Humphrey, *Introduction to the Team Software Process*, Addison-Wesley Professional, August 1999.
13. *ISO/IEC 12207:1995 Information Technology – Software life cycle processes*, ISO, Geneva 1995.
14. *ISO/IEC 15504:1998 (E) Information Technology – Software Process Assessment - Parts 1-9*, ISO, Geneva 1998.
15. *ISO/IEC 14143 Information Technology – Software measurement – Functional size measurement – Part 1-6*, ISO, Geneva 1998-2007.
16. *ISO/IEC 14598 Information Technology – Software Product Evaluation - Parts 1-6,* ISO, Geneva 1998-2001.
17. *ISO/IEC 9126 Software Engineering – Product Quality – Part 1-4,* ISO, Geneva 2001-2004.
18. *ISO/IEC 15288:2002 Systems engineering -- System life cycle processes*, ISO, Geneva 2002.
19. *ISO/IEC 20968:2002 Software engineering – Mk II Function Point Analysis - Counting practices manual,* ISO, Geneva 2002.
20. *ISO/IEC 9126-2:2003 Software Engineering – Product Quality – Part 2: External metrics*, ISO, Geneva 2003.
21. *ISO/IEC 9126-3:2003 Software Engineering – Product Quality – Part 3:*

Internal metrics, ISO, Geneva 2003.
22. *ISO/IEC 19761:2003 Software engineering – COSMIC-FFP – A functional size measurement method,* ISO, Geneva 2003.
23. *ISO/IEC 20926:2003 Software engineering - IFPUG 4.1 Unadjusted functional size measurement method - Counting practices manual,* ISO, Geneva 2003.
24. *ISO/IEC 9126-4:2004 Software Engineering – Product Quality – Part 4: Quality in use metrics*, ISO, Geneva 2004.
25. *ISO/IEC 90003:2004 Software Engineering – Guidelines for the application of ISO 9001:2000 to computer software*, ISO, Geneva 2004.
26. *ISO/IEC 24570:2005 Software engineering – NESMA functional size measurement method version 2.1 - Definitions and counting guidelines for the application of Function Point Analysis,* ISO, Geneva 2005.
27. *ISO/IEC 14143-1:2007(E) Information Technology – Software measurement – Functional size measurement – Part 1: Definition of concepts*, ISO, Geneva 2007.
28. *ISO/IEC 15939:2007 Systems and software engineering - Measurement process*, ISO, Geneva 2007.
29. *ITIL Lifecycle Publication Suite*, Office of Government Commerce, The Stationery Office (TSO), London, May 2007.
30. Johnson J., *CHAOS Rising*, The Standish Group International, Inc., Referat zaprezentowany na II-giej Krajowej Konferencji Jakości Systemów Informatycznych, Warszawa, czerwiec 2005.
31. R.S. Kaplan, D.P. Norton, *The Balanced Scorecard: Measures That Drive Performance*, Harvard Business Review, August 25, 2007.
32. M. Kasunic, *The State of Software Measurement Practice: Results of 2006 Survey*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, December 2006.
33. Kisielnicki J., Sroka H., *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Wyd. III zm., Placet, Warszawa 2005.
34. Kobyliński A., *Modele jakości produktów i procesów programowych*, Monografie i Opracowania 539, Oficyna Wydawnicza SGH, Warszawa 2005.
35. A. Kobyliński, T. Chodoła, *Pomiary w praktyce wytwarzania oprogramowania*, w: *Studia i materiały Polskiego Stowarzyszenia Zarządzania Wiedzą* nr 7, red. W. Bojar, L. Drelichowski, G. Dzieża, A. Januszewski, Bydgoszcz-Ciechocinek 2006.
36. W. Kopaliński, *Słownik języka polskiego*, Tom I, PWN, 1978.
37. W.L. Melo, *Enhancing Rational Unified Process for Capability Maturity Model Integration Compliance: A Methodological Approach*, white paper, Unisys Corporation, June 2006.
38. J. Oakland, *Statistical Process Control*, 6E edition, Butterworth Heinemann, September 2007.
39. R.E. Park, W.B. Goethert, W.A. Florac, *Goal-Driven Software Measurement – A Guidebook*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, August 1996.

40. *Practical Software and Systems Measurement: A Foundation for Objective Project Management, Version 4.0b,* U.S. Department of Defense and U.S. Army, October 2000.
41. Kevin Richins, *Measurement in CMMI*, Proceedings of a Seminar On Metrics, International Council on System Engineering (INCOSE), Hampton, Virginia, October 23-24, 2001.
42. Standish Group, *The CHAOS Report (1994),* West Yarmouth, Massachusetts, 1995.
43. Standish Group, *The CHAOS Chronicles III*, West Yarmouth, Massachusetts, 2003.
44. Standish Group, *The Standish Group Report 2007*, West Yarmouth, Massachusetts, 2007 (w przygotowaniu).

ROZDZIAŁ VI

KONIUNKTURA I DOSKONAŁOŚĆ – CZY TO JEST PARA?

Iwona D. BARTCZAK

Wygląda na to, że czasy koniunktury sprzyjają szaleństwu, łamaniu konwencji i ryzykownym projektom. Nie są to jednak projekty budowaniu doskonałego przedsiębiorstwa, super sprawnej organizacji, samonapędzających się mechanizmów innowacyjności i doskonalenia. Czy rola IT rośnie zatem w czasie koniunktury?

Jakie obszary mają największą szansę na zwiększenie poziomu informatyzacji w Pani/Pana firmie w wyniku przygotowań do Euro 2012 i ich realizacji?

Źródło: Business Dialog, maj 2007

Bardzo wielu analityków rynkowych, a zwłaszcza rynku IT, uważa, że wzrost koniunktury pociąga za sobą wzrost budżetów IT. Czy aby na pewno? A jeśli nawet, to czy te pieniądze są wydawane za trwałe ulepszenie firmy? Czy one będą procentowały w przyszłości? A może po prostu robi się absolutnie konieczne zakupy informatyczne odkładane w nieskończoność? Gdy tak się szczęśliwie składa, że firma – dokonując cudów rękami super inteligentnych informatyków - przetrwała bez tych zakupów do czasów koniunktury, to teraz może sobie na nie

pozwolić. Ale czy te zakupy budują przyszłość firmy?

Do tych rozważań skłoniły mnie badania, które w 2007 roku przeprowadziła moja firma, czyli wydawnictwo Business Dialog. A szczególnie wiele do namysłu dały mi wyniki majowych badań dotyczących Euro 2012 i budżetów IT. Uważamy dosyć powszechnie, że przygotowania i organizacja Euro wzmocni koniunkturę. Ale czy ten fakt wzmocni informatyzację firm?

Euro 2012 – w zasadzie bez znaczenia

Zdaniem zdecydowanej większości respondentów (83%) Euro 2012 nie wpłynie na wysokość budżetów IT, nawet jeśli ich firmy spodziewają się wzrostu albo utrzymania koniunktury w związku z tym wydarzeniem. Wyjaśnienie jest stosunkowo proste – i potwierdzają je inne badania Business Dialog – w czasach prosperity firmy nie podejmują w zasadzie działań naprawczych czy usprawniających firmę, procesy w niej czy produkty. Koncentrują się na zdobywaniu klientów, zwiększaniu udziałów w rynku. Natomiast inwestycje informatyczne kojarzone są raczej z modernizacją i wewnętrznymi udoskonaleniami. W tej sytuacji dobrą wiadomością jest przekonanie respondentów, że Euro 2012 nie spowoduje obniżenia budżetów na IT, że szefowie informatyki nie będą musieli rywalizować z szefami biznesowymi o środki finansowe w sposób bardziej zacięty niż dotychczas.

To zapatrzenie w rynek – a nie do wnętrza firmy – widać także z odpowiedzi na pytanie, jakie obszary mają największe szanse na zwiększenie informatyzacji w związku z Euro. Aż 83% respondentów wskazało sprzedaż i marketing, a 33% relacje z klientami. 50% respondentów spodziewa się, ze firmy położą nacisk na integrację procesów i automatyzację procesów administracyjnych. Ta ostatnia odpowiedź może wynikać z tego, że firmy liczą się z kłopotami kadrowymi. Wówczas automatyzacja i inne działania zmniejszające pracochłonność będą chętniej wdrażane. Na uwagę zasługuje też bezpieczeństwo danych, na co wskazało 33%.

66% szefów IT nie będzie używać argumentów związanych z Euro 2012 do walki o budżety. Wygląda na to, że Euro nie funkcjonuje jeszcze w biznesie jako coś więcej niż wydarzenie sportowe, ewentualnie możliwość pozyskania dodatkowych kontraktów, ale wcale nie jakiś szczególnie atrakcyjnych, nawet dla branży budowlanej, która woli budować biurowce i apartamentowce. Euro nie stanowi zupełnie impulsu do unowocześnień i innowacyjności, co jest najbardziej pożądane.

Mądrość w czasie koniunktury

Te odpowiedzi harmonizują z wynikami innego naszego badania (wraz z firmą HADATAP) z maja 2007. „Mądrość firm w czasach koniunktury: upraszczanie procesów i minimalizowanie strat".

Z tego badania wynika niezbicie, że największym dzisiejszym zagrożeniem

firm jest zaniedbywanie doskonalenia struktur i procesów wewnętrznych (67%), koncentracja na inwestycjach w zdobywanie rynku, kosztem wewnętrznych usprawnień (47%). W trzeciej kolejności wskazano zaniechanie unowocześniania zasobów produkcyjnych (40%), a jako czwarte - lekceważenie doskonalenia kwalifikacji kadry (33% odpowiedzi). Firmy doskonale wiedzą, że warto w czasie koniunktury inwestować w usprawnianie procesów i badania. Obie te pozycje wskazało po 60% respondentów. 53% wskazało modernizację zasobów produkcyjnych.

Paradoksem jest więc, że firmy wiedzą, jak powinny się zachowywać w czasie koniunktury, jakiej hierarchii celów przestrzegać, a jednak bardzo często tak nie czynią. Co jest przyczyną tego zjawiska? Brak wiedzy wewnątrz firmy? Brak motywacji do wyznaczania długofalowych celów? Interesy grup menedżerów i pracowników, które mogłyby być zagrożone w wyniku doskonalenia? W każdej firmie odpowiedź będzie inna, jednak samo zjawisko powinno pobudzić do działania właścicieli i rady nadzorcze oraz zarządów, pilnujących długoterminowych interesów całej firmy.

W badaniu szczególnie interesowano się procesem produkcyjnym. Po czym firmy poznają, że ten proces źle funkcjonuje? Przede wszystkim sygnalizuje im to niestabilna jakość produktów (60% odpowiedzi). Następnie równorzędny procent odpowiedzi uzyskały: wąskie gardła i spiętrzenia oraz trudności w synchronizacji procesu przy zwiększonej różnorodności produktów (47%). Zwracano również uwagę na nieterminowość wysyłek do klientów i brak informacji o produkcji w toku. Większość firm posiada systemy informatyczne wspomagające zarządzanie produkcją. Czy one źle wywiązują się ze swojego zadania? „Im więcej czasu mija od wdrożenia w przedsiębiorstwie zintegrowanego systemu informatycznego, tym bardziej rozwiązania biznesowe oddalają się od tego, co można osiągnąć przy pomocy nowszych technologii IT. Postęp w tej dziedzinie jest ogromny i pracownicy w firmie, mający wiele zadań, nie są w stanie na bieżąco śledzić nowych rozwiązań" – komentuje Zenon Parol, menedżer HADATAP. Jego opinie potwierdza odpowiedź menedżerów na pytanie ankiety o rolę systemów IT. Niemal wszyscy odpowiedzieli, że są użyteczne pod warunkiem, że systematycznie unowocześnia się je lub wymienia na bardziej odpowiadające biznesowi.

Na pytanie szczegółowe, jakie są najistotniejsze przyczyny strat, opóźnień i błędów w procesie produkcyjnym aż 80% respondentów wskazało brak współpracy w łańcuchu dostaw, 73% - niedoskonałość systemu planowania produkcji, a 60% opóźnienia w pozyskiwaniu istotnych informacji. Z praktyki najlepszych firm wynika, że eliminacja strat, opóźnień i błędów powinna być pierwszym działaniem usprawniającym funkcjonowanie firmy. Przeważnie daje to od razu znakomite rezultaty, a także jest punktem wyjścia do bardziej wyrafinowanych projektów doskonalenia i podnoszenia efektywności działania firmy.

„Rozkład odpowiedzi w poszczególnych pytaniach wskazuje, że prezesi i dyrektorzy generalni analizują pracę firmy, a więc pracę ludzi, w kategoriach skutku i wyniku, natomiast dyrektorzy operacyjni częściej widzą proces i jego

niedoskonałości. Większy potencjał jest w podejściu procesowym, ponieważ pracownicy uczestniczący w procesie mają realną możliwość zmieniania go, doskonalenia. Muszą jednak mieć do tego motywację i akceptację zwierzchników oraz poznać techniki ulepszania procesów." – twierdzi Andrzej Góralczyk, główny doradca produktywności, menedżer czołowego portalu menedżerskiego Dyrekcja.pl. Gromadzeniem wiedzy o biznesie i procesach powinni zajmować się pracownicy w firmie, ale wiedzę o metodykach, rozwiązaniach, narzędziach i trendach najlepiej kupić od zewnętrznych dostawców.

Dyrektorzy informatyki uczestniczący w badaniu generalnie zgadzają się w swoich opiniach z dyrektorami biznesowymi, jednak widać pewne charakterystyczne różnice. Po pierwsze, są bliżej procesów, więc widzą, że negatywne wyniki firmy, np. dotyczące zdobywania rynku czy niestabilna jakość produktów wynikają właśnie z błędów w sterowaniu procesem lub ustawieniu procesu. Szefowie IT nie są związani z praktyką produkcyjną, z operacjami, w związku z tym bardziej przejmują się niedoskonałym parkiem maszynowych, przestarzała technologią niż menedżerowie biznesowi nawykli do problemów wynikających stanu technicznego wyposażenia lub technologii.

Po drugie, szefowie biznesowi bardzo mocno akcentują znaczenie kwalifikacji kadry, zdobywanie utalentowanych pracowników i menedżerów. Są skłonni w to inwestować. IT chyba nie ma problemu z kompetencjami, dlatego nie widzi tego problemu.

Wydaje się, że jedni drugich mogą twórczo zainspirować. Menedżerowie odpowiedzialni za wyniki powinni dostrzec, że poprawia się jej umożliwiając ludziom dobrą pracę poprzez prawidłowe ustawienie procesu i sterowanie nim, a nie tylko przez presję na pracowników, aby zwiększali wysiłek. Menedżerowie IT natomiast dobrze, jakby nabyli nawyku upraszczania procesów i generalnie funkcjonowania firmy, szybkiego podążania do wyniku. Z dialogu między takimi dyrektorami mogą powstać bardzo skuteczne pomysły usprawniania firm.

„Mądrość firm w czasach koniunktury: upraszczanie procesów i minimalizowanie strat."

1. Jakie są najważniejsze zagrożenia czyhające na dobrze rozwijającą się firmę w czasach koniunktury, zagrożenia płynące z jej organizacji i systemu zarządzania?)

47%	**a. silna koncentracja na zdobywaniu udziałów w rynku i zwiększaniu sprzedaży, lekceważenie wewnętrznych usprawnień**
13%	b. rozdźwięk między rosnącym popytem a możliwością jego zaspokojenia w terminie
27%	c. lekceważenie jakości, gdyż „rynek i tak weźmie wszystko"
67%	**d. zaniedbanie doskonalenia struktur i procesów wewnętrznych**

33%	**e. lekceważenie doskonalenia kwalifikacji kadry**
40%	**f. zaniechanie inwestycji w unowocześnianie technologii produkcyjnych**
7%	g. spowolnienie rozwoju systemów wsparcia biznesu
20%	h. niska motywacja do innowacyjności
13%	i. brak umiejętności lub niechęć do ujawniania strat i błędów
7%	j. wewnętrzne słabości, które nie pozwalają wykorzystać wszystkich okazji rynkowych

2. W co najlepiej inwestować podczas dobrej koniunktury?

20%	a. marketing i promocję
20%	b. infrastrukturę i kadrę handlową
20%	c. nowe produkty
53%	**d. modernizację zasobów produkcyjnych**
27%	e. systemy informatyczne wspierające biznes
60%	**f. usprawnianie procesów biznesowych**
60%	**g. badania i rozwój**
20%	h. pozyskanie dobrej kadry menedżerskiej i specjalistów
13%	i. szkolenie

Źródło: Business Dialog, maj 2007

O co więc chodzi?

Menedżerowie zapytani o ten fenomen mają różne interpretacje. Tomasz Kibil, dyrektor IT w Polkomtelu (kończący właśnie swoją misję w tej firmie) zadaje fundamentalne pytanie o to, czy firmy mają strategię – na gorsze i na lepsze czasy – czy po prostu biorą, co życie przynosi. „Podejrzewam, że Euro 2012 traktują jak napad na bank, skok na kasę, jak kolejną okazję do zarobienia, a nie czynnik rozwoju." Łukasz Koska z Warbudu broni branży budowlanej, też niespecjalnie entuzjastycznie nastawionej do Euro 2012, mówiąc że inne rodzaje budownictwa są znacznie bardziej rentowne niż budowa stadionów. Nie ukrywa też, że nie zostało zdefiniowanych tyle warunków formalnych, prawnych, infrastrukturalnych, że po prostu nie można jeszcze w biznesplanach brać pod uwagę mistrzostw. Paweł Kiełczykowski, dyrektor finansowy i administracyjny Schenker uważa, że można zmobilizować kolegów z zarządu do perspektywicznego myślenia pokazując, czym się różni zarządzanie kosztami od cięcia kosztów. „Oczywiście zarządzanie kosztami trzeba zacząć w czasach

koniunktury, bo w kryzysie już się nie da nimi zarządzać, trzeba ciąć, zwykle na oślep." Konrad Kobylecki, dyrektor operacyjny Polkomtel mówi, że oszczędności uzyskane dzięki usprawnieniom wewnętrznym nigdy nie wyniosą tyle, ile dodatkowe przychody z nowych sprzedaży. Dlatego inwestycje się w IT, które wzmacnia sprzedaż, a nie to które przynosi oszczędności. Natomiast korzyści długofalowe nie są brane pod uwagę w rachunku ekonomicznych w czasach koniunktury.

Ale najbardziej zainspirowało mnie przypuszczenie finansisty Olgierda Bagniewskiego. „Być może firmy są jak organizmy żywe poddane ewolucji. Przekształcają się dopiero wtedy, gdy muszą, w ostatniej chwili. Gdy wszystko idzie dobrze, nie mają motywacji do zmian. Gdy idzie źle mają taką motywację, ale nie mają środków do przeprowadzenie zmian, nie mają czasu, nie mają optymizmu ludzi. Przekształcają się, żeby przetrwać, ale tylko troszeczkę, na ile im skromne środki pozwalają." Czy to dobrze czy źle. Może dobrze? Przecież jeśli przekształcimy się tylko troszeczkę, to jest bardzo małe ryzyko, że popełnimy błąd. Nie wykonamy zapewne wielkiego skoku. Ale przetrwamy. Może to jest najważniejsze?

CZĘŚĆ 2

ZASTOSOWANIA

ROZDZIAŁ VII

ZASTOSOWANIE NARZĘDZI INFORMATYCZNYCH ORAZ TECHNOLOGII RFID W ŁAŃCUCHU LOGISTYKI ODWROTNEJ

Janusz GRABARA, Aleksandra NOWAKOWSKA

Wstęp

Logistyka odwrotna powinna być postrzegana jako kompleksowe działania obejmujące nie tylko ponowne użycie opakowań i recykling materiałów służących do pakowania, ale przede wszystkim jako proces przemieszczania się dóbr z przeznaczenia końcowego do punktu powstania w celu odzyskania wartości lub prawidłowego zagospodarowania. Kompleksowość działań w zakresie logistyki odwrotnej wymusza poszukiwanie rozwiązań informatycznych służących optymalizacji przepływów i lepszego zarządzania procesem zwrotów w łańcuchu logistyki odwrotnej.

Informatyczne wspomaganie przepływu zwrotnego

Konkurencyjny rynek wymusza poszukiwanie obszarów działalności firmy, w których można dokonać redukcji kosztów działań. Takim obszarem, służącym uzyskaniu przewagi rynkowej, mogą być zwroty produktów. Nie będzie możliwa racjonalizacja przepływu zwrotnego bez odpowiednich informacji i danych, a co za tym idzie systemu zarządzania nimi. Wszelkie działania logistyczne opierają się na informacjach uzyskiwanych z różnych baz danych usystematyzowanych i zarządzanych poprzez systemy informatyczne. Dane istotne z punktu widzenia logistyki odwrotnej, które poddawane są przetwarzaniu muszą być właściwie uzyskiwane z zewnątrz, przechowywane i przekazywane na zewnątrz systemu. Przepływ ten wspomagany jest systemami informatycznymi, bez których współcześnie realizowana logistyka byłaby niewydolna[1]. Systemy ERP (*Enterprise Resource Planning)*, które wspomagają przedsiębiorstwo głównie w sferze planowania, produkcji i dystrybucji zbudowane są z szeregu aplikacji zapewniających integrację poszczególnych obszarów działalności przedsiębiorstwa. Przynoszą liczne korzyści dla działań biznesowych. Do kilku głównych można zaliczyć:

- rozszerzenie możliwości wykorzystania informacji w sposób wielokrotny bez ryzyka utraty ich aktualności i przejrzystości,
- integrację poszczególnych rozproszonych jednostek organizacyjnych przedsiębiorstwa i ułatwienie zarządzania nimi na rynku globalnym,

[1] Majewski J., *Informatyka dla logistyki,* Wyd. ILiM, Poznań 2006

- wpływ na wzrost znaczenia systemów informatycznych dla przedsiębiorstwa, które nie pełnią już wyłącznie funkcji pomocniczych, lecz służą kompleksowo realizacji działań operacyjnych, jak i strategicznych mających na celu poprawę konkurencyjności przedsiębiorstwa na rynku,
- zminimalizowanie trudności występujących w dotychczasowych systemach, które były mniej elastyczne. Systemy klasy ERP są dopasowywane do indywidualnych potrzeb przedsiębiorstwa,
- wyjście naprzeciw użytkownikom, duża liczba pracowników mająca dostęp do systemu przyczynia się do zwiększenia jego przejrzystości i ułatwienia tym samym korzystania z dostępnych danych[2].

Współczesne systemy ERP są ściśle zintegrowane z innymi systemami. Z punktu widzenia logistyki odwrotnej na uwagę zasługują systemy CRM, w których J. Witkowski wyróżnia charakterystyczne moduły, takie jak[3]:

- Moduły analityczne:
  - Analiza i planowanie akcji promocyjnych
  - Prognozowanie sprzedaży
  - Segmentacja rynku i klientów
- Moduły komunikacyjne:
  - Zarządzanie korespondencją
  - Telemarketing
  - Telekonferencje
  - Przekaz danych między centralą a przedstawicielami w terenie
- Moduły operacyjne:
  - Bazy danych o klientach i transakcjach
  - Sporządzanie ofert z indywidualizacją warunków transakcji
  - Rejestrowanie zamówień i oczekiwań klientów
  - Monitorowanie statusu klientów
  - Raportowanie sprzedaży
  - Obsługa klientów

W łańcuchu dostaw zwrotnych konieczne jest określenie warunków dla towarów lub materiałów, które pozwalają przyjąć lub odrzucić zwrot na wejściu do systemu. Jeśli odnosi się to do zwrotów, to koncepcja jest bardziej złożona. Ważne i celowe staje się zdobycie szczegółowych, powiązanych danych o zwrotach w punkcie rozpoczynającym przepływ, aby możliwe stało się właściwe nimi rozporządzanie. W punkcie decyzyjnym następuje synteza wiedzy na temat całości zwrotów, która może zostać opublikowana z wyszczególnieniem elementów składowych, takich jak: jakość, łańcuch dostaw, obsługa klienta, obsługa posprzedażna. Ta funkcja pojawia się w określonym momencie i miejscu, gdzie następuje autoryzacja przedmiotu zwrotów (*Returns Material Authorization*) i zwrot jest przydzielany do odpowiedniej osoby, na przykład dystrybutora, klienta, sprzedawcy. Istotne jest tutaj wskazanie różnicy pomiędzy zdolnościami do

[2] Pr. zbiorowa pod red. M. Ciesielskiego, *Instrumenty zarządzania logistycznego*, PWE Warszawa 2006.

[3] Witkowski J., *Zarządzanie łańcuchem dostaw*, PWE Warszawa 2003.

prostego przedstawiania w RMA (co wiele systemów może robić) i zdolności do zatwierdzania poszczególnych elementów w trakcie procesu wbrew z góry ustalonym zmiennym (co może zrobić niewiele systemów).

Działania w zakresie logistyki odwrotnej wspierane są przez zaawansowane rozwiązania techniczne i informatyczne, przede wszystkim są to rozwiązania klasy SCM powiązane coraz częściej z technologią radiowej identyfikacji. Korzystanie z narzędzi informatycznych usprawnia powiązania z innymi podmiotami, na przykład na drodze outsourcingu.

W przypadku zlecania działań logistycznych partnerom 3PL (*Third Part Logistics* - operatorom logistycznym) działania w zakresie logistyki odwrotnej również muszą uwzględniać ten fakt. Przepływy zwrotne dotyczą czterech typów podmiotów w sieci dostaw: producent kontraktowy, odbiorca finalny, pośrednik i kooperant, które są koordynowane i prowadzone przez operatora 3PL. Można wskazać również na przepływy informacyjne, jakie w związku z takimi zdarzeniami są realizowane: informacje płyną od producenta kontraktowego za pośrednictwem operatora 3PL do właściciela marki i produktu.

W rozwoju współczesnej logistyki obserwowane są tendencje do przyznawania istotnej roli procesom przepływu informacji w łańcuchu dostaw. Konieczne jest poszukiwanie sposobów skutecznego zarządzania tym obiegiem,co staje się możliwe dzięki rozwojowi nowych technologii, do których zalicza się RFID, czyli Radio Frequency Identification. Jest to system identyfikacji towarów oparty na technologii umożliwiającej transmisję danych pomiędzy tagiem (elektroniczną etykietą, chipem, transponderem), a czytnikiem za pomocą fali radiowych. Działa na podobnej zasadzie, co technologia kodów kreskowych, ale daje dużo większe możliwości. Pozwala ona na bardzo dużą automatyzację pracy związanej z odczytywaniem danych, jest wygodna i łatwa w użyciu. Do cech wyróżniających ją spośród dotychczas wykorzystywanych technologii zdalnej identyfikacji można zaliczyć:

- stosunkowo dużą odporność na warunki zewnętrzne, takie jak: kurz, zmiany temperatur, opady wstrząsy, wibracje, promieniowanie słoneczne
- wytrzymałość na uszkodzenia mechaniczne większa niż w tradycyjnych kodach kreskowych
- brak konieczności bezpośredniego kontaktu pomiędzy tagiem a czytnikiem, dzięki czemu istnieje możliwość umieszczenia tych elementów w sposób niewidoczny
- możliwość odczytu informacji z więcej niż jednego obiektu jednocześnie z zabezpieczeniem ich przed kopiowaniem i utraceniem
- gwarancję niskiego poziom błędu transmisji danych.
- zwiększona ilość informacji o produktach, dane te są dynamiczne ponieważ przedsiębiorstwo może dokonywać zmian w systemie informatycznym.
- bezpieczeństwo informacji o produkcie, standardowe kody kreskowe zawierają informacje, które mogą być odczytane przez każdego. Standard RFID pozwala na przechowywanie danych w systemie, do którego dostęp można umożliwić określonej grupie upoważnionych użytkowników

Rozwój technologii RFID przebiega w szybkim tempie, warto więc wskazać na cechy odróżniające stosowane transpondery między sobą, jednym z nowszych stosowanych są tagi pasywne bez zasilania o dużym zasięgu odczytu i aktywne- mające własny system zasilania[4]. Zapotrzebowanie na rynku występuje zarówno na tagi aktywne zasilane bateryjnie o zasięgu odczytu 30m, kosztujące od 10 do 150 USD za sztukę, jak i tagi pasywne krótkiego zasięgu (0,3-0,6) m w cenie 1 USD za sztukę. Wśród czynników decydujących o jakości działania można wymienić następujące parametry:

- czułość tagów, parametr ten decyduje o możliwościach zasilenia układu scalonego i uzyskanej dzięki temu sile sygnału emitowanego w stronę czytnika, a tym samym o wielkości zasięgu.
- rozmiar tagów- im większy tym większy zasięg
- kształt tagów- kształt anteny wpływa na zasięg działania.
- liczba anten podłączonych do układu scalonego. Dwie anteny dipolowe podłączone do jednego układu scalonego zapewniają mniejszą wrażliwość na kierunek działania. Ma to duże znaczenie, kiedy odczyt odbywa się z różnych kierunków.
- szybkość powiązana z wydajnością, z jaką czytnik pozyskuje identyfikatory tagów. Większa szybkość pozwala uzyskać dokładniejszy odczyt i zmniejsza obciążenie.
- gęstość tagów- tagi umieszczone w niewielkiej odległości mogą wzajemnie zakłócać swoje działanie.
- materiał nośny- przy zastosowaniu materiałów zawierających wodę i metale mogą wystąpić zakłócenia w odczycie. Sposobem na ich zminimalizowanie jest stosowanie separatorów między tagiem a oznakowanym produktem, np. tektury, tworzyw sztucznych.

Przy uwzględnieniu wyżej wymienionych czynników możliwe jest zastosowanie skutecznych elementów systemu RFID. Z rozwiązań RFID mogą korzystać zarówno producenci, jak i dystrybutorzy i sprzedawcy detaliczni. Pionierami jej stosowania są wielcy detaliści, jak na przykład Wal-Mart, Best Buy i Target w USA, Metro, Tesco w Europie. Amerykańska sieć hipermarketów Wal-Mart zobowiązała swoich stu największych dostawców do zainteresowania się tą techniką już kilka lat temu. Obecnie kolejni dostawcy implementują systemy RFID dla produktów, które trafiają do sieci handlowej Wal-Mart. Systemy RFID działają również w armii amerykańskiej, były m.in. wykorzystywane do nadzorowania operacji logistycznych podczas wojny w Iraku.W codziennym życiu stosowane są podobne rozwiązania, np. system nawigacji satelitarnej umożliwiający optymalne przebycie trasy z punktu A do B, oglądanie dowolnego miejsca na świecie z lotu ptaka za pomocą Google Earth. W łańcuchu logistyki odwrotnej dzięki RFID każdy produkt z osobna jest możliwy do identyfikacji. Hala magazynowa zostaje przeskanowana dla zlokalizowania produktów tracących ważność, które powinny zostać wyrzucone lub wycofane ze sprzedaży i zwrócone do producenta lub

[4]Grabara J., Kot S., *RFID- nowe możliwości usprawnienia przepływu dóbr*, [w:] Informacja i komunikacja w logistyce, Katowice 2005

przesłane pośrednikowi. Natomiast w przypadku kiedy produkt jest zwracany przez klienta możliwe jest sprawdzenie historii dostawy, gdzie, kiedy i jak ten produkt został kupiony i wykrycie ewentualnego oszustwa, a następnie wyeliminowanie go, czyli obniżenie tym samym kosztów serwisu[5]. W ten sam sposób gdy wadliwe produkty zwracane są na podstawie gwarancji historia ich przepływu zostaje pokazana w formie zestawienia. Zarówno pośrednik, jak i producent uzyskują w ten sposób natychmiastową informację o odsetku zwrotów towarów i mogą zdiagnozować przyczyny wadliwości produktów, jak również opracować plan działania, np. podjąć decyzję o wycofaniu partii wyrobów. Możliwa staje się redukcja kosztów dzięki zmniejszeniu poziomu zapasów, jak i zapewnieniu cykliczności dostaw, można precyzyjniej określić terminy dostaw, redukując tym samym koszty transportu. Lepsza komunikacja w łańcuchu daje możliwość uzyskania bardziej aktualnych i dokładniejszych analiz popytu i dostosowania do nich właściwej polityki zapasów i planowania produkcji. Osiągana jest większa skuteczność w relacjach z dostawcami poprzez harmonogramowanie dostaw, poprawia się czas reakcji na nagłe zmiany popytu i podaży. Przedsiebiorstwo może również lepiej zarządzać aktywami, np minimalizując koszty przestoju i utrzymania maszyn i urządzeń.Technologia RFID otwiera ogromne możliwości innowacji wewnątrz dużych organizacji o złożonych procesach logistycznych. Opłacalność zastosowania tej technologii wzrasta szczególnie gdy firma:

- posiada liczny asortyment produktów
- ma zakłady o dużej powierzchni i rozproszonej lokalizacji
- obejmuje liczne miejsca składowania
- odbywają się w niej częste ruchy magazynowe- występuje duża rotacja materiałów, produktów, opakowań
- ma dodatkowe wymagania i potrzeby informacyjne wynikające ze specyfiki branży, np. terminy przydatności, identyfikacja partii surowców.

Właściwie zaplanowane i skoordynowane działania w wymienionych obszarach pomagają w minimalizowaniu strat zarówno dla klientów, którym nie zapewniono należytego poziomu obsługi, jak również dla przedsiębiorstwa, które marnotrawi swoje zasoby dostarczając wadliwych produktów. Jest to szczególnie widoczne w przypadku zwrotów towarów zwracanych do producenta w celu naprawy lub z powodu pomyłek w wysyłce. Zastosowanie rozwiązań z zakresu radiowej identyfikacji pozwala zminimalizować możliwość wystąpienia niedociągnięć w obsłudze. Technologia ta umożliwia monitorowanie produktów na poziomie palet i skrzyń, które przenoszone są przez bramki RFID w punkcie przyjmowania lub wysyłki towarów, a także w wewnętrznych punktach kontrolnych, co pozwala na zarejestrowanie i nadzór nad wszelkimi ruchami kontrolowanych pozycji asortymentowych. Uzyskanie kompleksowej informacji przyczynia się do usprawnienia przepływu produktów, będą one dostarczane w odpowiednim czasie i miejscu. Ograniczone zostaną przypadki zgubienia, czy kradzieży towarów, zmniejszenie braków w asortymencie, zwiększenie lojalności

[5] Wyld D.C., *The RFID Value Proposition for Reverse Logistics: Part II RFID In Action*, Reverse Logistics Magazine March/April 2007

klienta i w końcowym efekcie zwiększenie przychodów i zyskowności. Na uwagę zasługuje również udział identyfikacji w przepływie, takich elementów, jak:

- *Zwrotne opakowania transportowe,* takie jak palety, kratki, kontenery. Są one istotne z punktu widzenia procesów logistycznych, (czasem zdarza się, iż nie wracają z powrotem w oryginalnym stanie), mogą one być wykorzystane ponownie do dalszego transportowania innych towarów do miejsca przeznaczenia.
- *Opakowania zwrotne detaliczne*, jak na przykład butelki czy puszki. Te produkty zwykle wymagają mycia i doprowadzenia do stanu używalności i mogą być ponownie wielokrotnie użyte.
- *Materiały do recyklingu,* takie jak tonery do kserokopiarek i cartridge do drukarek, monitory telewizyjne, papier i tym podobne. Są to produkty, które straciły swoją funkcjonalność. Ich odzyskiwanie jest zwyczajowo narzucane przedsiębiorstwom przez ustawy dotyczące ochrony środowiska. Najczęściej w recyklingu tych materiałów odzyskuje się metale i takie części, które mogą być ponownie użyte. Odzyskane składniki są ponownie używane przez przedsiębiorstwa, które je skupiły, bądź są wykorzystywane dla celów przemysłowych w innych branżach.
- *Zwroty,* dotyczą na przykład pozycji, których nie było w specyfikacji, pozycje dostarczone zbyt późno i tak dalej. Osoby, które zamawiają produkty przez Internet, często dokonują zwrotów wynikających z tego, iż dobra oglądane na ekranie komputera mogą wyglądać inaczej, niż w rzeczywistości, przez co ich nie satysfakcjonują. Czasem też dobra o wysokim zaawansowaniu technologicznym, takie jak na przykład monitory komputerowe zostają uszkodzone w trakcie transportu, co powoduje, że nie nadają się w pełni do dalszego wykorzystania i muszą zostać zwrócone do producenta.
- części zamienne, materiały z odzysku, odrzuty, materiały niewykorzystane i inne.
- Z rozwiazań RFID mogą korzystać wszyscy uczestnicynłańcucha dostaw: zarówno producenci, jak i dystrybutorzy i sprzedawcy detaliczni, możliwe staje się zwiększenie efektywności współpracy w całym łańcuchu dostaw. Szczególnie z osiągnięć identyfikacji radiowej mogą korzystać przedsiębiorstwa o złożonych procesach logistycznych, mające liczne asortymenty produktów, posiadające zakłady o dużej powierzchni i rozproszonej lokalizacji.

Wskazując na liczne zalety technologii RFID, nie można zapomnieć o jej niedoskonałościach. W przypadku tagów starszej generacji takim ograniczeniem są koszty, często zbyt duże w stosunku do możliwości finansowych przedsiębiorstwa. Nie bez znaczenia są również wymagania techniczne stawiane krajom Unii Europejskiej przez ETSI (European Telecommunication Standard Institute), które różnią się od standardów przyjętych w Stanach Zjednoczonych i innych krajach świata, co ogranicza możliwość korzystania z rozwiązań zastosowanych poza UE.

Podsumowanie

Działania logistyki odwrotnej nie mogą być realizowane bez zastosowania

właściwych narzędzi informatycznych. Złożoność przepływów informacyjnych, które wiążą się z procesami logistyki odwrotnej, powoduje konieczność wybrania odpowiednich narzędzi systemowych. Przykładem mogą być narzędzia w typie Workflow, których wykorzystanie warunkuje prawidłowość procesów przepływu towarów w łańcuchach dostaw. Wydaje się, że wraz z rozwijaniem sfery obsługi klienta w przedsiębiorstwach i podnoszeniem przez to swojej pozycji konkurencyjnej działania z zakresu przepływów zwrotnych także będą udoskonalane tak, aby klient w najlepszy sposób został usatysfakcjonowany. Jednocześnie potrzeba dostosowania działań przedsiębiorstw do coraz bardziej proekologicznego prawodawstwa w zakresie zagospodarowania zwrotów towarów, także wymusi na przedsiębiorstwach konieczność zastosowania systemów informacyjnych, które będą w stanie sprostać nowym wyzwaniom. Należy podkreślić znaczącą rolę technologii RFID, dzięki której możliwe jest stworzenie prawdziwego, globalnego łańcucha dostaw. Działania w zakresie logistyki odwrotnej, wymagają bezwzględnie nowych rozwiązań systemowych w zakresie identyfikacji towarów wycofanych z użytku i skierowanych do powtórnego przerobu, bądź też przygotowywanych do innego zagospodarowania. Dzięki zastosowaniu technologii RFID możliwe jest zgromadzenie takiej ilości informacji, która pozwala na bardzo dokładne śledzenie przepływu zwrotnego, a to jest bardzo przydatne dla prawidłowego budowania łańcuchów dostaw zwrotnych. Organizacją, która działa na rzecz globalnego łańcucha dostaw w przyszłości jest EPCglobal. Jej aktywność koncentruje się na ujednolicaniu standardów technologicznych poprzez wpływ na rozwój RFID w dwóch kierunkach. Z jednej strony jej działania zmierzają do unifikacji danych w taki sposób, aby były odczytywalne w każdym miejscu na świecie, z drugiej strony proponuje globalne standardy komunikacji pomiędzy tagiem a czytnikiem, czyli protokoły RFID.

Powszechnie obserwowana integracja w ramach odwrotnego łańcucha dostaw powoduje konieczność rozbudowy systemów informatycznych, tak aby był możliwy łatwy dostęp do informacji i szybki ich przepływ zarówno od klienta przez firmę do dostawcy, jak i w odwrotnym kierunku. Rozwój systemów informatycznych wspomagających funkcjonowanie przedsiębiorstw przyczynił się w znaczący sposób do optymalizacji wewnętrznych procesów biznesowych, czyli usprawnienia funkcjonowania poszczególnych ogniw łańcucha i efektywnego przepływu informacji pomiędzy nimi.

Literatura

1. Eurologistics nr 2/2006
2. Eurologistics nr 3/2006
3. Grabara J., Kot S., *RFID- nowe możliwości usprawnienia przepływu dóbr*, [w:] Informacja i komunikacja w logistyce, Katowice 2005
4. Majewski J., *Informatyka dla logistyki,* Wyd. ILiM, Poznań 2006
5. Pr. zbiorowa pod red. M. Ciesielskiego, *Instrumenty zarządzania logistycznego*, PWE Warszawa 2006.
6. Witkowski J., *Zarządzanie łańcuchem dostaw*, PWE Warszawa 2003.

7. Wyld D.C., *The RFID Value Proposition for Reverse Logistics: Part II RFID In Action*, Reverse Logistics Magazine March/April 2007

ROZDZIAŁ VIII

PARAMETRYCZNY SPOSÓB OCENY DOSTĘPNOŚCI INFORMACJI W ORGANIZACJI GOSPODARCZEJ

Andrzej M. MICHALSKI

Wprowadzenie

W organizacjach gospodarczych informacja należy do najważniejszych zasobów. Bezpieczeństwo posiadanej i wymienianej informacji ma bezpośredni wpływ na osiąganie przychodu z prowadzonej działalności, zachowanie płynności finansowej oraz kreowanie pozytywnego wizerunku marketingowego (pozycji na rynku) [CERTYF07]. Wynika z tego, że niezbędna jest właściwa polityka ochrony informacji. Opublikowana w 2005 roku norma ISO 27001, dotycząca zarządzania bezpieczeństwem informacji [INFORM05], wyróżnia trzy podstawowe obszary (płaszczyzny), które składają się na bezpieczeństwo informacji, a mianowicie poufność, integralność i dostępność. Każdy z tych obszarów wymaga stosowania odpowiednich metod i technologii. W niniejszym opracowaniu autor postanowił skupić się na zagadnieniu dostępności informacji. Równocześnie zwiększający się udział informacji jako składnika kosztów produktu finalnego oraz duża dynamika procesów produkcyjnych [MICHAL98], [SIEJAC98] stanowią obiektywne przesłanki wykorzystania w działalności przedsiębiorstwa systemu informatycznego zarządzania [DAMGAA02], ponieważ przetwarzanie znacznych ilości informacji jest możliwe do osiągnięcia jedynie poprzez wspomaganie komputerowe.

1. Informacja i jej dostępność

We współczesnych warunkach zarządzania organizacją gospodarczą dostępność informacji (zasobów informacyjnych) nabiera kluczowego znaczenia i podstawowym sposobem, mającym ją zapewnić, jest wdrożenie systemu informatycznego [CALLAG02], [WYKORZ02]. Wtedy dostępność informacji traktować możemy zarówno jako stan, jak i cechę systemu informatycznego organizacji. Pod pojęciem dostępności informacji w niniejszym opracowaniu rozumie się taki stan (taka cechę) systemu informatycznego organizacji, który (która) zapewnia uprawnionemu użytkownikowi zaspokojenie każdego poprawnie sformułowanego żądania dostępu do informacji w czasie, wynikającym z realizowanych procesów biznesowych. Na rozwiązania, związane z zapewnieniem dostępności informacji w organizacji mają wpływ cele i potrzeby tej organizacji, wymagania bezpieczeństwa, realizowane procesy biznesowe, wielkość i struktura samej organizacji a także wdrożony system informatyczny.

Uwarunkowania, związane z systemem informatycznym przedsiębiorstwa, to projekt i realizacja sieci komputerowej, wybór metod i narzędzi zdalnego dostępu do zasobów informacyjnych, zapewnienie nieprzerwanego przetwarzania danych, zabezpieczenie zasobów informacyjnych przed wpływem czynników zewnętrznych, działania organizacyjne, związane z zapewnieniem ciągłości procesów biznesowych po awarii lub katastrofie, i wreszcie wykorzystanie nowych technologii sprzętowych i programowych, ułatwiających zapewnienie dostępności informacji.

Dostępność informacji można rozpatrywać na dwóch poziomach: ogólnym i szczegółowym. Poziom ogólny dotyczy analizy dwóch zagadnień:

1. Przygotowanie środowiska sprzętowego i programowego, umożliwiającego realizację czterech podstawowych procesów informacyjnych (pozyskiwania, przechowywania, przetwarzania i udostępniania informacji).
2. Zapewnienie zabezpieczenia tego środowiska przed skutkami złych działań (na poziomie sprzętowym, programowym i organizacyjnym).

Poziom szczegółowy związany jest z przeanalizowaniem konkretnej aplikacji w świetle określonych procesów biznesowych. Do tego etapu odnieść możemy ustalenie:

- jakie będą potrzebne informacje, wymagane przez procesy, (czy zaprojektowane struktury danych zapewniają możliwość uzyskania potrzebnej informacji);
- kto z tych informacji będzie korzystał (czy przygotowane są profile użytkowników, posiadających stosowne uprawnienia);
- czy dostępność informacji skorelowana jest z procesami biznesowymi (czyli analiza czasowa dostępności informacji na żądanie).

Zwykle ostatni z wymienionych punktów jest najbardziej krytyczny.

Z powyższego wywodu wynika, że móc aby odpowiedzieć menedżerowi na temat dostępności konkretnej informacji w konkretnym systemie obsługującym konkretne procesy należy dokonać analizy konkretnego przypadku (w rzeczywistym czasie i środowisku).

I jeszcze jedna istotna kwestia - zależność pomiędzy danymi i informacją. W [MANAGI96] możemy znaleźć, że informacja, to zestrukturyzowane dane, czyli dane, które zostały uporządkowane: zdefiniowano kategorie informacji i każdy fakt został odniesiony do odpowiedniej kategorii. Z tego wynika, że wystarczającym procesem, umożliwiającym przekształcenie danych w informację jest porządkowanie (bez konieczności ich przetworzenia). Takie podejście zostało wybrane przez autora pracy do prowadzenia dalszych rozważań. Jest to o tyle istotne, że zarówno z punktu widzenia bezpieczeństwa, jak i dostępności, pojęcia danych i informacji możemy traktować ekwiwalentnie, tzn. bezpieczeństwo informacji zapewnimy, gwarantując bezpieczeństwo danych i ich spójność, a dostępność informacji jest zagwarantowana przez dostępność odpowiednich danych, przechowywanych we właściwej bazie danych.

2. Sposoby oceny dostępności

W wielu publikacjach technicznych, jak np. [BEZPIE06], [KOBYLI05], [RELIAB06], [SYSTEM06], [WIELKA05], oraz w materiałach normatywnych, jak to ma miejsce np. w omawianej już normie ISO 27001 [INFORM05], dostępności informacji traktowana jest jako jeden z elementów bezpieczeństwa lub niezawodności systemu, stąd też potrzeba posiadania jakiegoś mierzalnego kryterium do jej wyrażenia. Gdyby za [KOBYLI05] przyjąć, że dostępność (gotowość) jest atrybutem przybliżonym do niezawodności i określenia te bywają używane wymiennie, wówczas w oparciu o [ALBINS03], [BASCLE98] i [FENPFL97] dostępność można wyrazić jako procent czasu, w którym system jest sprawny, w postaci następującej zależności:

$$A = \frac{MTTF}{MTTF + MTTR} \times 100\%$$

gdzie A - dostępność (ang. Availability),
$MTTF$ - średni czas pomiędzy rozpoczęciem pracy a chwilą utraty przez system sprawności (ang. Mean Time To Failure),
$MTTR$ - czas niedostępności, związany z czasem, niezbędnym na naprawę i przywróceniem stanu gotowości (ang. Mean Time To Repair).

I chociaż tak zdefiniowany miernik dostępności uwzględnia różne czynniki zewnętrzne, jak np. konsekwencje awarii, jednakże brakuje mu istotnej cechy - nie uwzględnia powiązania z realizowanymi procesami biznesowymi, jak np. wymagany czas reakcji.

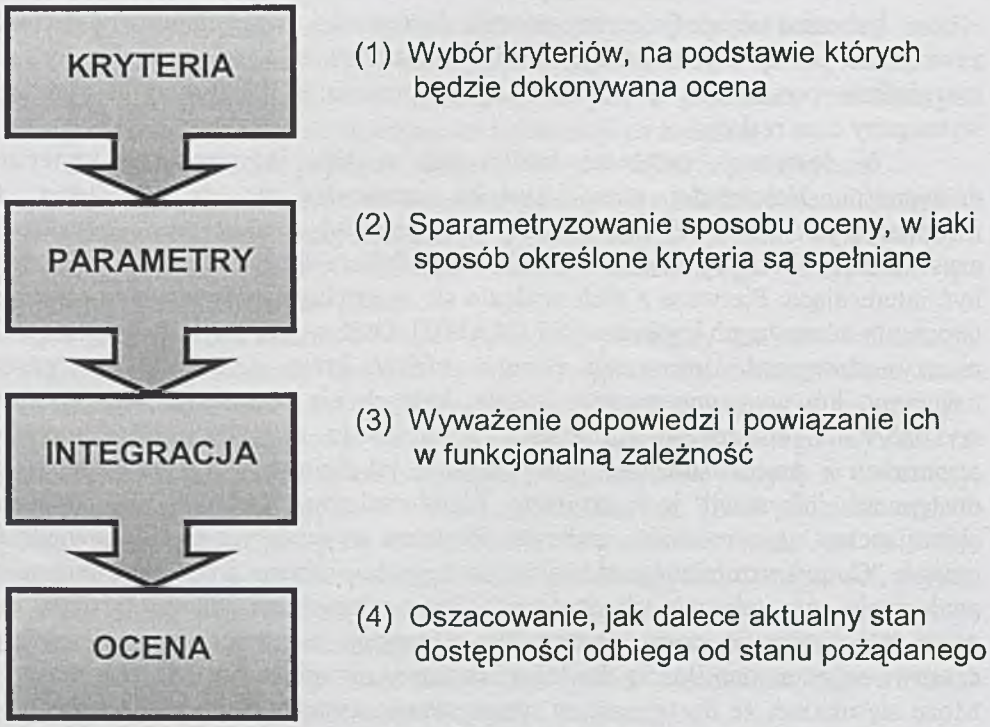
W dostępnej literaturze trudno jest znaleźć informacje o kryteriach dostępności. Najczęściej charakterystyka sprowadza się do określenia, że informacja jest mniej czy też bardziej dostępna (lub niedostępna). Jednakże w czasie analizy literatury autor zauważył dwa podejścia, które w tym aspekcie mogą być interesujące. Pierwsze z nich znalazło się w artykule, poświęconym tendencji tworzenia mierzalnych kryteriów [SYSKAE03]. Otóż w tym artykule proponuje się mierzyć dostępność informacji poprzez efekty, które dzięki tej dostępności osiągamy, lub wyrażone poprzez koszty, których nie ponosimy. Jako przykład wykorzystano dostępności informacji w systemie zarządzania dokumentami organizacji i przeciwstawiane jest podejście jakościowe (gdy przyjmiemy, że dostępność informacji jest aktywem niemierzalnym) podejściu ilościowemu, opierającemu się o mierniki liczbowe. Punktem wyjściowym jest odpowiedź na pytanie "Co jest rozumiane pod hasłem dostępności informacji?" I następnie próba znalezienia ocen mierzalnych przy znalezieniu odpowiedzi, jak np. dostępnością może być skrócenie czasu dostępu do informacji, a wtedy już same różnice czasowe są mierzalną ilością dla której możemy przypisać wartość ekonomiczną. Może się okazać, że dostępność w tym systemie oznacza również, że informacja rzadziej ulega zagubieniu. To także jest mierzalne; np. wtedy gdy ta informacja wpływa na rutynowe decyzje podejmowane w firmie. Potrafimy wówczas znaleźć ekonomiczną wartość tego usprawnienia poprzez pomiar efektów zredukowania

kosztownych błędów utraty tej informacji. Lepsza dostępność informacji skutkuje tym, że mniej jest sytuacji, kiedy utrata informacji powoduje dodatkowe koszty związane z jej odtworzeniem (jak na przykład: powtórne wykonanie rysunków inżynierskich, ponieważ oryginały zaginęły). Czyli zawsze możemy sprowadzić to pojęcie do czegoś konkretniejszego, a przez to mierzalnego.

Drugim podejściem jest ocena parametryczna, zaproponowana przez firmę Hewlett-Packard [BUSINE06] i wykorzystywana w narzędziu, służącym do oceny stanu bezpieczeństwa i dostępności informacji w przedsiębiorstwie i pozwalającym planować działania, zmierzające do poprawy tego stanu.

3. Parametryczny sposób oceny dostępności informacji

Na dostępność informacji w organizacji możemy wpływać poprzez mechanizmy techniczne (sprzęt i oprogramowanie) oraz organizacyjne (planowanie i procedury). Zaproponowano ekspercką parametryczną ocenę dostępności informacji na podstawie zintegrowanego kryterium ilościowego. Metoda ta posiada strukturę modułową (rys. 1), co pozwala w łatwy sposób dostosowywać ja do konkretnych okoliczności i rozwijać w miarę potrzeb. Każdy z modułów, będący kolejnym etapem przeprowadzanej oceny, wykorzystuje wyniki, uzyskane wcześniej, ale nie zależy funkcjonalnie od poprzednika.



Rys. 1. Parametryczna metoda ocena dostępności informacji [Opracowanie własne]

Do takiej oceny na etapie 1 może zostać wykorzystany np. zestaw kryteriów opracowanych w formie ankiety przez firmę Hewlett-Packard jako Business Continuity and Availability Self-Assessment Tool i obejmujący 26 pytań, lub zbiór rozszerzony, o którym mowa w [GAŁACH05] który zawiera ponad 790 pytań. Na każde z pytań należy udzielić jednej z odpowiedzi: "[Tak|Nie|Częściowo|Nie wiem]".

W dalszej części artykułu rozważania dotyczyć będą "krótkiej listy", czyli zbioru 27 kryteriów, sporządzonego przez autora na bazie [BUSINE06]. Lista kryteriów ma następującą postać:

1. Czy zidentyfikowano, które z procesów biznesowych są najważniejsze i przez jakie zasoby infrastruktury informatycznej są wspierane?
2. Czy zostały określone zagrożenia i niebezpieczeństwa zagrażające krytycznym procesom i zasobom informatycznym?
3. Czy zostały określone parametry ilościowe wpływu awarii lub zniszczenia krytycznych elementów infrastruktury informatycznej na prowadzoną działalność biznesową? Uwzględnić należy zarówno koszty bezpośrednie, jak utrata zamówień, przestoje pracowników, jak i koszty pośrednie: reputacja na rynku, zdolność kredytowa, kurs akcji na giełdzie.
4. Czy zostały zdefiniowane parametry, związane z odtwarzaniem systemu po katastrofie, a mianowicie czas, niezbędny na odtworzenie systemu (RTO) i dopuszczalny poziom utraty aktualnych danych (RPO)?
5. Czy zostały określone poziomy dostępności krytycznych usług infrastruktury informatycznej, które są niezbędne do zapewnienia właściwej realizacji procesów biznesowych?
6. Czy zostały przygotowane plany działań w sytuacjach nagłych zagrożeń (kryzysowych), których celem jest zarządzanie w takich sytuacjach i wznowienie procesów biznesowych?
7. Czy przeprowadzane są regularnie weryfikacje planów działań w sytuacjach kryzysowych, związane ze wszystkimi obszarami działalności przedsiębiorstwa (a nie np. tylko z zasobami informatycznymi)?
8. Czy istnieje udokumentowany plan zapewnienia ciągłości usług informatycznych (odtwarzania systemu po katastrofie)?
9. Czy plan zapewnienia ciągłości usług informatycznych uwzględnia obsługę systemów i urządzeń zabezpieczeń?
10. Czy plan zapewnienia ciągłości usług informatycznych przewiduje procedury, które winny być podjęte w przypadku dużych zniszczeń (np. gdy pomieszczenia nie będą mogły być dostępne przez czas dłuższy niż np. 45 dni)?
11. Czy odpowiednie umowy zapewniają wsparcie najważniejszych kooperantów w przypadku korzystania z nowej lokalizacji, w której odtwarzany jest system po katastrofie?
12. Czy istnieje regularnie weryfikowana jasna umowa serwisowa, gwarantująca odpowiedni poziom obsługi?

13. Czy realizowane są pełne zabezpieczenia (ang. backup) danych wszystkich krytycznych zasobów informatycznych systemu jako część zdefiniowanej strategii zabezpieczenia i odtwarzania danych?
14. Czy wszystkie krytyczne dane są dublowane np. w zapasowym systemie, czy to drogą zdalnej replikacji, czy też wykorzystując nośniki taśmowe?
15. Czy realizowane są zabezpieczenia danych na taśmach magnetycznych i czy te zabezpieczenia przechowuje się w oddalonych lokalizacjach?
16. Czy są regularnie realizowane testy posiadanych w oddalonych lokalizacjach zabezpieczeń danych drogą ich odtwarzania w systemie?
17. Czy posiadane plany zapewnienia ciągłości usług informatycznych są na bieżąco aktualizowane w celu uwzględnienia zmian i aktualizacji wprowadzanych do infrastruktury czy też instalacji nowych aplikacji w wyniku ich włączenia do ogólnych procedur zarządzania zmianami?
18. Czy są zdefiniowane w sposób jasny i jednoznaczny procedury wsparcia w przypadku sytuacji awaryjnych (ang. helpdesk), ukierunkowane na konkretne działania zmierzające do rozwiązania problemu?
19. Czy istnieje udokumentowana procedura zgłaszania awarii i problemów do dostawców usług serwisowych, w odniesieniu do zasobów krytycznych także poza normalnymi godzinami pracy?
20. Czy zostało zaimplementowane pełne monitorowanie środowiska pracy serwerów (pomieszczenia komputerowego)?
21. Czy pomieszczenie komputerowe jest zabezpieczone przed fluktuacjami lub zanikiem napięć zasilających, np. przez UPS?
22. Czy istnieje rezerwowa infrastruktura (np. linie analogowe), zapewniająca łączność w przypadku awarii krytycznych linii lub urządzeń komunikacyjnych?
23. Czy wykorzystuje się strukturę klastra lub inne formy redundancji w celu zapewnienia odporności na zagrożenia i awarie, na poziomie, gwarantującym realizację procesów biznesowych?
24. Czy infrastruktura przechowywania danych i wykonywania ich zabezpieczeń spełnia wymagania odnośnie dostępności informacji, uwarunkowanej procesami biznesowymi, a także wymogami RTO/RPO odtwarzania po katastrofie?
25. Czy przeprowadzane są regularne testy macierzy dyskowych i przechowywanych na nich danych w celu upewnienia się, że urządzenia pracują właściwie?
26. Czy istnieje i działa zautomatyzowany system, wykrywający stany odbiegające od normy i pojawiające się stany zagrożeń bezpieczeństwa, w celu alarmowania obsługi?
27. Czy istnieje udokumentowany proces eskalacji problemów w przypadku sytuacji trudnych i kryzysowych, kiedy nie można na miejscu znaleźć rozwiązania?

Jeżeli przeanalizujemy powyższe kryteria, to możemy zauważyć, że po pierwsze określają one bezpośrednio zespół metod i środków zapewnienia bezpieczeństwa informacji w przypadku awarii lub katastrofy. Po drugie,

podlegające ocenie przedsięwzięcia mogą zostać sklasyfikowane zarówno pod kątem obszaru funkcjonalnego, jak i znaczenia (ważności) dla zapewnienia dostępności. W zakresie funkcjonalności można wydzielić następujące obszary:

- identyfikacja czynników,
- przedsięwzięcia, zapewniające bezpieczeństwo informacji,
- procedury awaryjne.

Natomiast w odniesieniu znaczenia, czy też ważności kryterium, można wydzielić następujące poziomy przedsięwzięć:

- konieczne (niezbędne),
- pożądane,
- wspomagające.

Omówiona klasyfikacja może być przedstawiona w postaci układu macierzowego (tabelarycznego), w którym kolumny odpowiadają obszarom funkcjonalności, a wiersze poziomom ważności (Tabela 1). W tabeli każde kryterium przedstawione jest w formie numeru z przedstawionej wcześniej listy.

Tabela 1. Klasyfikacja kryteriów dostępności informacji

Funkcjonalność / Ważność	Identyfikacja	Bezpieczeństwo	Awaryjne
Konieczne	1,2,3,4,5,	6,7,12,13,21,23,24	8,9
Pożądane	-	14,15,16,17,22	10,11,19,25
Wspomagające	-	20	18,26,27

Źródło: Opracowanie własne

Taka klasyfikacja pozwala przejść do sporządzenia zintegrowanego kryterium oceny.

4. Zintegrowane kryterium oceny

Udzielenie rzetelnych odpowiedzi na sformułowane pytania to dopiero początek procesu. W dalszej kolejności należy dokonać oceny stopnia przygotowania organizacji (a przede wszystkim działu IT) do zapewnienia dostępności informacji, najlepiej mając do dyspozycji w miarę obiektywną metodę nie tylko jakościową, ale i ilościową. W tym celu autor proponuje wykorzystać zintegrowaną metodę oceny stanu przygotowania do zapewnienia dostępności informacji, niezbędnej do realizacji procesów biznesowych. Proponowana metoda

oceny opiera się o punktowany system odpowiedzi. W pierwszej kolejności odpowiedziom należy przyporządkować określone wartości punktowe (na podstawie wiedzy eksperckiej). Dobrym odwzorowaniem rzeczywistości wydaje się być następująca struktura punktów (Tabela 2):

Tabela 2. Wartości punktowe odpowiedzi

Odpowiedzi	*Punkty*
Tak	1
Częściowo	0,5
Nie	0,2
Nie wiem	0

Źródło: Opracowanie własne

Kolejny etap związany jest z wprowadzeniem w każdym obszarze funkcjonalnym odpowiednich wag, które wyrażają ważność określonego kryterium. Na podstawie posiadanego doświadczenia autor proponuje następujący układ (Tabela 3):

Tabela 3 . Wagi grup kryteriów

	Waga
Konieczne	0,5
Pożądane	0,3
Wspomagające	0,2

Źródło: Opracowanie własne

Przeprowadzone ustalenia pozwalają uzyskać wyrażoną liczbowo ocenę (miarę) dostępności informacji w realnych warunkach w odniesieniu do realizowanych procesów biznesowych. Taka ocena uzyskiwana jest w dwóch krokach. Krok pierwszy to wyliczenie rzeczywistej wartości dostępności (kryterium dostępności) według wzoru:

$$A = \sum_{j} (w_j \times \sum_{i} p_{ij})$$

gdzie A - wyliczona dostępność
p_{ij} - wartość punktowa odpowiedzi, dotycząca konkretnego kryterium
w_j - waga określonego poziomu ważności
i - kolejne kryterium w ramach poziomu ważności j
j - grupa kryteriów o określonym poziomie ważności

Krok drugi służy do oceny, jak bardzo stan aktualny odbiega od stanu, w którym zrealizowane są wszystkie niezbędne przedsięwzięcia, zapewniające dostępność informacji. Ocena ta realizowana jest w odniesieniu do maksymalnej

wartości, którą można uzyskać przy przyjętym systemie wartości punktów i wag. Wykorzystywana jest w tym celu następująca zależność:

$$P = \frac{A_{rzecz}}{A_{\max}} \times 100\%$$

gdzie P - aktualny poziom dostępności
A_{rzecz} - rzeczywista wartość wyliczonej dostępności
A_{max} - maksymalna wartość dostępności przy przyjętych kryteriach; np. przy wartościach, jak w tabelach 1, 2 i 3 $A_{max} = 10,5$.

Podsumowanie

Zaproponowana integralna miara dostępności informacji może być wykorzystywana jako jeden z elementów oceny przygotowania infrastruktury informatycznej organizacji gospodarczej do wymagań, związanych ze skutecznym procesem wspomagania procesu decyzyjnego i jego odporności na szkodliwe oddziaływania zewnętrzne.

Należy podkreślić, że zarówno zaproponowany sposób oceny dostępności, jak i otrzymane z jego pomocą konkretne wartości mają charakter bardzo przybliżony i w praktyce winny być wykorzystywane przez menedżerów służb informatycznych jedynie do oceny przygotowania infrastruktury informatycznej organizacji do zapewnienia dostępności informacji w ramach realizowanych procesów biznesowych i identyfikacji obszarów, wymagających poprawy.

Literatura

1. ALBINS03- Albin S. T.: The Art of Software Architecture - Design Methods and Techniques, Wiley Publishing, Indianapolis 2003.
2. BASCLE98 - Bass L., Clements P., Kazman R.: Software Architecture in Practice, Addison-Wesley, 1998.
3. BEZPIE06 Bezpieczeństwo informacji, Jason MacKenzie, 2006, http://jmk.pl/jmk/u9.html.
4. BUSINE06 - Business Continuity and Availability Self-Assessment Tool, Hewlett-Packard Company, http://h30328.www3.hp.com/ui/forms/Default.aspx, 2006.
5. CALLAG02 - Callaghan J.: Inside Intranets & Extranets: Knowledge Management and the Struggle for Power, Palgrave Macmillan, UK 2002.
6. CERTYF07 - Certyfikacja ISO 27001 - Zarządzanie bezpieczeństwem informacji, ISOQUAR CEE Sp. z o.o., portal www.isoquar.pl, Warszawa 2007.
7. DAMGAA02 - Damgaard J.: IT On the Fast Track, Optimize Magazine, September 2002.

8. FENPFL97 - Fenton N.E., Pfleeger S.L.: Software Metrics. A Rigorous and Practical Approach, 2nd ed., PWS Publishing Company, Boston 1997.
9. GAŁACH05 - Gałach A.: Zarządzanie bezpieczeństwem systemu informatycznego – uniwersalna lista kontrolna, Ośrodek Doradztwa i Doskonalenia Kadr Sp. z o.o., Gdańsk 2005.
10. INFORM05 - Information technology - Security techniques - Information security management systems - Requirements, International Standard ISO/IEC 27001, ISO/IEC 2005.
11. KOBYLI05 - Kobyliński A.: Modele jakości produktów i procesów programowych, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Warszawa 2005.
12. MANAGI96 - Managing Information, "Color In Color Out" CD, Epson, 1996.
13. MICHAL98 - Michalski A.: Uwarunkowania stosowania systemów informatycznych w przedsiębiorstwie, Materiały Konferencyjne Katedry Informatyki i Ekonometrii, Politechnika Śląska, Gliwice 1998.
14. RELIAB06 - Reliability and Availability Basics, EventHelix.com, http://www.eventhelix.com/RealtimeMantra/FaultHandling/reliability_availability_basics.htm, 2006.
15. SIEJAC98 Sierpińska M., Jachna T.: Ocena przedsiębiorstwa według standardów światowych, wydanie drugie, Wydawnictwo Naukowe PWN, Warszawa 1998.
16. SYSKAE03 - Syska E.: ROI: Wszystko jest mierzalne, IT Investment Consulting, http://www.it-invest ment.com.pl/index.php?option=com_content&task=view&id=84&Itemid=109, 2003.
17. SYSTEM06 -System pojąć a ludzi zrozumieć - recepta na udane wdrożenie, Portal rozwiązań IT w biznesie ERP-view.pl, www.erp-view.pl/ERP/system_poj_a_ludzi_zrozumie_-_recepta_na_udane_wdro_enie__2.html, sierpień 2006.
18. WIELKA05 - Wielka Internetowa Encyklopedia Multimedialna 2006, Onet.pl. 2005.
19. WYKORZ02 - Wykorzystanie technologii i systemów informatycznych w procesach decyzyjnych, praca zbiorowa pod red. Andrzeja Michalskiego, Wydawnictwo Politechniki Śląskiej, Gliwice 2002.

ROZDZIAŁ IX

WSPOMAGANIE GOSPODAROWANIA ODPADAMI KOMUNALNYMI SYSTEMEM INFORMATYCZNYM

Marta STAROSTKA-PATYK

Zwiększające się corocznie ilości odpadów komunalnych i przemysłowych w Polsce stają się coraz większym problemem natury zarówno ekonomicznej jak i społecznej. Dlatego odpowiednie zorganizowanie gospodarowania odpadami ma bardzo istotne znaczenie.

Odpadem jest każdy materiał powstały w wyniku działania człowieka lub przyrody, jako niezamierzony ale trudny do uniknięcia skutek. Odpad nie może być użytkowany w ogóle lub w pełni ze swoim pierwotnym przeznaczeniem w danym miejscu i czasie[1]. Ze względu na miejsce powstawania odpadów dzielone są one na: komunalne, przemysłowe i niebezpieczne. Odpady komunalne powstają w wyniku bytowania człowieka, odpady przemysłowe w wyniku prowadzenia działalności gospodarczej. Odpady niebezpieczne w przeważającej większości są jednocześnie odpadami przemysłowymi[2].

Tabela 1 przedstawia charakterystykę ilościową odpadów wytwarzanych w Polsce w latach 1990 – 2005, gdzie przedstawiono ilość ogólną odpadów oraz ich ilości w rozbiciu na poszczególne rodzaje.

Tabela 1. Odpady wytworzone w ciągu roku. (bd – brak danych).

ODPADY [tys. ton]	1990	1995	2000	2001	2002	2003	2004	2005
Komunalne	11 098	10 985	12 226	11 109	10 509	9 925	9 759	9 354
Przemysłowe	143 861	122 662	125 484	123 810	117 894	120 551	124 004	124 602
Ogółem	154 959	133 647	137 710	134 919	128 403	130 476	133 763	133 956
Niebezpieczne	bd	bd	1 601	1 308	1 029	1 339	1 349	1 779

Źródło: opracowanie własne na podstawie danych GUS.

Powyższe zestawienie ukazuje rosnącą tendencję ilościową odpadów.

[1] P. Ambrożewicz „Zwarty system zagospodarowywania odpadów", Wyd. Ekonomia i Środowisko, Białystok 1999.

[2] Ustawa o odpadach, Dz. U. z 1997, nr 96, poz. 592.

Mimo, że ilość odpadów komunalnych po roku 2000 corocznie ulega niewielkiemu obniżeniu[3], to ilości odpadów przemysłowych i niebezpiecznych w ostatnich latach wzrastają, co jest przyczyną corocznego wzrostu ogólnej ilości odpadów.

Analizując odpady komunalne należy przybliżyć źródła ich powstawania. Są to przede wszystkim gospodarstwa domowe, a także różnorodne obiekty infrastruktury działające w sferze handlu, usług i rzemiosła, szkolnictwa czy turystyki[4].

Biorąc pod uwagę źródła wytwarzania odpadów komunalnych oraz analizując ich skład z punktu widzenia możliwości technologicznych związanych z odzyskiem i unieszkodliwianiem odpadów wyodrębniono strumienie odpadów[5]:

- odpady organiczne (domowe odpady organiczne pochodzenia roślinnego lub zwierzęcego ulegające biodegradacji oraz odpady pochodzące z pielęgnacji ogródków przydomowych, kwiatów domowych, balkonowych – ulegające biodegradacji),
- odpady zielone (odpady z ogródków i parków, targowisk, z pielęgnacji zieleńców miejskich, z pielęgnacji cmentarzy – ulegające biodegradacji),
- papier i karton (opakowania z papieru i tektury, opakowania wielomateriałowe na bazie papieru),
- tworzywa sztuczne (opakowania z tworzyw sztucznych),
- tekstylia,
- szkło (opakowania ze szkła),
- metale (opakowania z blachy stalowej, opakowania z aluminium, pozostałe opakowania metalowe),
- odpady mineralne – odpady z czyszczenia ulic i placów: gleba, ziemia, kamienia itp.,
- drobna frakcja popiołowa – odpady ze spalania paliw stałych w piecach domowych (głównie węgla), z uwagi na udział w składzie odpadów komunalnych popiołu wyodrębniono te frakcję jako nieprzydatną do odzysku i unieszkodliwiania innymi metodami poza składowaniem,
- odpady budowlane – odpady z budowy, remontów i demontaży obiektów budowlanych – w części wchodzące w strumień odpadów komunalnych,
- odpady wielkogabarytowe,
- odpady niebezpieczne wytwarzane w grupie domowych odpadów komunalnych.

Wszystkie te strumienie odpadów komunalnych można scharakteryzować wskaźnikami wedle ich ilości i jakości, uwzględniając różnice ich powstawania na terenie zabudowy miejskiej i wiejskiej, co prezentuje tabela 2.

---

[3] Wynika to z większej dbałości władz miast i gmin o środowisko naturalne, propagowania ochrony środowiska naturalnego i rosnącej świadomości społecznej

[4] S. Kot „Supply Chain Management in Global Scale". W:Financni a logisticke rizeni - 2007. Sbornik referatu z mezinarodni konference. Malenowice, Ceska republika 2007

[5] J. Bendkowski, M. Wengierek „Logistyka Odpadów. Procesy logistyczne w gospodarce odpadami", Wyd. Politechniki Śląskiej, Gliwice 2002.

Tabela 2. Strumienie odpadów komunalnych na terenach miejskich i wiejskich w 2003 roku w kg/M/r (kg na mieszkańca rocznie).

Strumienie odpadów komunalnych	Miasto [kg/M/r.]	Wieś [kg/M/r.]
Odpady kuchenne ulegające biodegradacji	90,20	22,11
Odpady zielone	10,00	4,16
Papier i tektura (nieopakowaniowe)	26,62	10,64
Papier i tektura	41,52	10,64
Opakowania wielomateriałowe	4,66	1,73
Tworzywa sztuczne (nieopakowaniowe)	48,27	21,03
Opakowania z tworzyw sztucznych	15,53	6,77
Tekstylia	12,10	4,65
Szkło (nieopakowaniowe)	2,00	1,00
Opakowania ze szkła	28,12	18,89
Metale	12,79	4,55
Opakowania z blachy stalowej	4,57	1,63
Opakowania z aluminium	1,33	0,47
Odpady mineralne	14,30	13,25
Drobna frakcja popiołowa	46,70	40,28
Odpady wielkogabarytowe	20,00	15,00
Odpady budowlane	40,00	40,00
Odpady niebezpieczne	3,00	2,00
Razem	423,71	223,59

Źródło: opracowanie własne na podstawie danych IETU

Wszystkie wyżej przedstawione informacje pokazują jak istotny jest problem odpowiedniego gospodarowania odpadami komunalnymi za względu na ich duże nagromadzenie. Jednocześnie coraz bardziej zaostrzane są przepisy regulujące ochronę środowiska naturalnego, gdzie kładziony jest duży nacisk na poprawną organizację procesu gospodarowania odpadami[6]. Gospodarowanie odpadami oznacza zbieranie, transport, odzysk i unieszkodliwianie odpadów, jak również nadzór nad tymi działaniami i miejscami unieszkodliwiania odpadów[7]. Taka formuła definicji jednoznacznie określa, że proces gospodarowania odpadami rozpoczyna się już w miejscu ich wytworzenia i kończy w momencie ich definitywnego unieszkodliwienia. Dzięki takiej rozpiętości może on przebiegać wielokierunkowo w zależności od rodzaju zagospodarowywanych odpadów lub

[6] S. Kot „B2B Exchanges-opportunity for Purchasing Process". Elektronnoe modelirovanie T.29 nr 4, 2007

[7] ustawa o odpadach ustawa z 27.04.2001 r. art. 3 ust. 3 pkt 1

form ich zagospodarowania[8].

Przedsiębiorstwa zajmujące się gospodarowaniem odpadami coraz częściej korzystają ze specjalnych systemów informatycznych, które wspomagają ich działalność. W celu zobrazowania gospodarki odpadami komunalnymi z wykorzystaniem wspomagającego systemu informatycznego można przedstawić przykład spółki X gospodarującej odpadami komunalnymi w Częstochowie[9]. Firma należy do grupy działającej w sektorze ochrony środowiska. Jej działalność jest podzielona na trzy podstawowe obszary: zbiórka i transport odpadów, zagospodarowanie odpadów oraz oczyszczanie. Spółka kieruje swoją ofertę zarówno do klientów indywidualnych jak i instytucjonalnych.

Jej system informatyczny oparty jest na programie fakturująco-rozliczeniowym RUOM (Rozliczanie Usług Oczyszczania Miasta). Jego podstawowa część funkcjonuje jako rozwiązanie typu CRM, czyli Zarządzanie Relacjami z Klientem.

Podstawowa część programu opiera się na istocie funkcjonowanie rozwiązań typu CRM (Customer Relationship Management). Ponieważ firma obsługuje klientów zgodnie z normami ISO 9001:2000 oraz ISO 14001:1996 działanie systemu informatycznego umożliwia zagwarantowanie najlepszej jakości obsługi klientów, gdyż obsługuje procesy związane z marketingiem, sprzedażą, rozliczeniem i reklamacją w obrębie wszystkich kanałów komunikacji z klientami, jak również dokładne analizy stanowiące podstawy procesu podejmowania decyzji. Pozwala także na bezproblemową integrację z innymi modułami tego systemu oraz z oprogramowaniem innych dostawców dzięki spersonalizowanemu dostępowi do informacji o kliencie.

Integralną częścią systemu jest Moduł Eksploatacji. Umowy (i aneksy) zawarte z klientami są tu danymi wejściowymi, natomiast dane wyjściowe stanowią wstępnie pogrupowane informacje będące jednocześnie danymi wejściowymi do pozostałych modułów. To oznacza że ten moduł służy do wprowadzania danych do systemu. W nim każdy klient posiada własną kartotekę zawierającą podstawowe informacje związane z zawartą umową takie jak: sposób rozliczania usług, rodzaj i wielkość pojemnika, częstotliwość i dni wywozu odpadów. Klienci są identyfikowani w systemie poprzez automatycznie nadawane numery komputerowe. Taka organizacja umożliwia pracownikom Biura Obsługi Klienta do szybkiego udzielenia klientom informacji o które poprosi on w danym momencie. Możliwe jest również śledzenie zmian umowy poprzez funkcję archiwizacji w systemie.

Korzystając z modułu eksploatacji, system pozwala uprawnionym osobom na rozliczanie klienta ze świadczonych mu usług w module Fakturującym. Tutaj program samodzielnie rozpoznaje rodzaje świadczonych usług i przypisuje ich wartość do odpowiednich grup rodzajowych. Względem rozliczeń system

---

[8] K. Gruszecki „Administracyjnoprawne ograniczenia działalności gospodarczej dotyczące składowania odpadów", GLOSA Prawo gospodarcze w orzeczeniach i komentarzach, nr 11, 2002.

[9] Analiza przypadku przeprowadzona na podstawie informacji udzielonych przez Spółkę X

wykazuje dużą elastyczność dla sposobu rozliczeń, co pozwala rozliczać klientów np. ze względu na ilość wywożonych pojemników, ilość osób zamieszkujących w gospodarstwie domowym, ustaloną kwotę ryczałtową itp. Faktura na życzenie klienta może zostać wydrukowana syntetycznie dla określonej ilości osób lub pojemników, albo analitycznie dla pojedynczych posesji. Może zostać również wykorzystany algorytm pozwalający na wydruk faktury za dowolny okres, jednocześnie blokując wielokrotne naliczanie płatności.

System wyposażony jest także w moduł Rozliczeniowy, który jest odpowiedzialny za rozliczenia finansowe między firmą a klientem. Pozwala to pracownikom na sprawdzanie bieżącego salda klienta, daty dokonania określonych wpłat czy też wysokości naliczanych odsetek od nieterminowych opłat. Funkcjonuje tu system indywidualnych kont bankowych generowanych przez specjalny algorytm automatyzujący procesy księgowania i eliminujący błędy księgowe. Konta bankowe są drukowane bezpośrednio na fakturach. Dzięki temu klient zyskuje pewność, że dokonana opłata jest księgowana na jego konto.

Dokumenty wprowadzone i wygenerowane w systemie wykorzystywane są w module Kontrolingu. Moduł ten kontroluje fakturowanie i płatności oraz analizuje dane zawarte w systemie na użytek pracowników i zarządu.

W przedsiębiorstwie dane z systemu wykorzystywane są przez Dział Eksploatacji. Możliwe jest generowanie kart brygadowych dla ekip wywozowych ze szczegółowym planem obsługiwanych posesji. Na podstawie tych danych i możliwości porównania ich na przestrzeni dowolnego okresu można porównać obciążenie nakładem pracy brygad i w razie potrzeby dokonać korekt. Pracownicy mogą też sporządzać raporty z czasowo wstrzymanych na wniosek np. klienta, realizacji umów. Służy to optymalizacji dziennej trasy brygad.

Z systemu korzysta także Dział Księgowości w celu sprawdzenia zaległości w opłatach wybranych grup klientów. Można również sprawdzić nierozliczone faktury i w przypadku rozpoczęcia działań windykacyjnych poprzez pracowników Spółki lub firmy zewnętrzne zostaje przekazana informacja do działu Eksploatacji o konieczności rozwiązania umowy o świadczenie usług.

Wszelkiego rodzaju analizy i raporty generowane w systemie wykorzystywane są przez Zarząd Spółki. Porównanie obrotów w grupach działalności daje możliwość wstępnego nakreślenia kierunku rozwoju firmy. Te raporty i analizy pozwalają na zobrazowanie bardziej i mniej rentownych przedsięwzięć, jak również tendencje zmian. Dodatkowo w celu zwiększenia efektywności RUOM posiada możliwość przeniesienia i dalszej analizy danych w programie Excel, co jest wygodnym i popularnym rozwiązaniem w systemach informatycznych.

Przedsiębiorstwa gospodarujące odpadami i wykorzystujące systemy informatyczne w celu wspomagania tego procesu mogą oczekiwać wielu korzyści z tego wynikających. Dzięki rozwiązaniom informatycznym możliwe jest uzyskanie przewagi konkurencyjnej wynikającej z posiadania obszernej wiedzy o klientach i otoczeniu biznesowym, wzrostu lojalności klientów czy zwiększonej zdolności firmy do reagowania na zmieniające się warunki rynkowe. Przedsiębiorstwa mogą też zwiększyć przychody poprzez koncentrację na bardziej rentownych klientach,

efektywne pozyskiwanie nowych klientów, ukierunkowanie na sprzedaż usług dodatkowych i sprzedaż droższych produktów oraz na wyższe wskaźniki sukcesu będące efektem zastosowania marketingu bezpośredniego. Możliwe jest także obniżenie kosztów przez intensyfikację wszelkich procesów, redukcję opłat administracyjnych, skoordynowane działania sprzedaży czy lepsze planowanie reklamy i marketingu bezpośredniego. Dodatkowym atutem są możliwości analityczne, które stanowią podstawę procesu planowani i podejmowania decyzji.

Również klienci korzystają z tego, że firma gospodarująca odpadami komunalnymi posiada system informatyczny. Oferta i zakres działalności są bardziej dostosowane do potrzeb klienta, możliwy jest kontakt wykorzystujący różne formy komunikacji jak internet, fax, e-mail, Biuro Obsługi Klienta czy opcje obsługi bezpośredniej, a także wyższy poziom świadczenia usług poprzez zindywidualizowaną obsługę klienta, szybsze przetwarzanie zleceń, jednolitą formę informacji czy komunikacji.

Efektem stosowania systemów informatycznych w przedsiębiorstwach gospodarujących odpadami komunalnymi jest przede wszystkim większa efektywność postępowania z odpadami i osiąganie korzyści w postaci większej dbałości o środowisko naturalne.

Literatura

1. P. Ambrożewicz „Zwarty system zagospodarowywania odpadów", Wyd. Ekonomia i Środowisko, Białystok 1999.
2. J. Bendkowski, M. Wengierek „Logistyka Odpadów. Procesy logistyczne w gospodarce odpadami", Wyd. Politechniki Śląskiej, Gliwice 2002.
3. K. Gruszecki „Administracyjnoprawne ograniczenia działalności gospodarczej dotyczące składowania odpadów", GLOSA Prawo gospodarcze w orzeczeniach i komentarzach, nr 11, 2002.
4. S. Kot „B2B Exchanges-opportunity for Purchasing Process". Elektronnoe modelirovanie T.29 nr 4, 2007
5. S. Kot „Supply Chain Management in Global Scale". W:Financni a logisticke rizeni - 2007. Sbornik referatu z mezinarodni konference. Malenowice, Ceska republika 2007
6. Ustawa o odpadach, Dz. U. z 1997, nr 96, poz. 592.
7. Ustawa o odpadach ustawa z 27.04.2001 r. art. 3 ust. 3 pkt 1

ROZDZIAŁ X

ZARZĄDZANIE LOGISTYCZNO-MARKETINGOWE W ŁAŃCUCHACH DOSTAW

Joanna NOWAKOWSKA – GRUNT

Skala makroekonomiczna problemów logistycznych obejmuje wszelkie zagadnienia związane z przepływem dóbr w całych gospodarkach. Przedsiębiorstwa działają na rynku współpracując ze sobą w tworzeniu całych łańcuchów logistycznych łączących ze sobą producentów, przedsiębiorstwa zaopatrujące i dystrybutorów w jeden, kompleksowy system, którego zadaniem jest jak najsprawniejsze przeprowadzenie procesów przepływu dóbr w celu zaspokojenia potrzeb klienta. Ponieważ następuje powszechna globalizacja gospodarki, świat staje się „totalną wioską", zagadnienia związane z przepływem dóbr w takim organizmie także nabierają specjalnego znaczenia. Budowa mniej lub bardziej skomplikowanych łańcuchów logistycznych wymaga spełnienia określonych warunków, przede wszystkim z zakresu wskazania możliwej integracji działań w obrębie rozbudowanych łańcuchów logistycznych. Obecnie bacznie zwraca się uwagę na logistykę jako funkcję przekrojową, a także przejaw procesów dostosowawczych, wymaganych do zrealizowania w przedsiębiorstwach chcących podjąć wyzwania międzynarodowe.

Trendy rozwoju światowego rynku ujawniają się głównie w procesach postępującej globalizacji działalności gospodarczej, w coraz większej różnorodności produktów oraz ciągłym skracaniu cyklu ich życia. Szybki rozwój zaawansowanych technologii informatycznych oraz coraz szersze procesy integracyjne przedsiębiorstw nie uznają granic ani barier językowo-kulturowych. W tej sytuacji wysoka jakość towarów i ich cena nie są jedynymi determinantami gwarantującymi efektywność sprzedaży. Coraz częściej decyduje o tym czas i poziom obsługi klienta. Przedsiębiorstwa uczestniczące w łańcuchu dostaw dążą do skracania czasu przepływu towarów i informacji, redukcji kosztów, a także zwiększania efektywności działań. Wynikiem owych dążeń ma być podniesienie poziomu obsługi klientów. Dążenie do większej efektywności działania, lepszej obsługi klienta, a także skuteczniejszej reakcji na zmieniającą się sytuację na rynku, zmusza przedsiębiorców do podejmowania szeregu działań usprawniających funkcjonowanie łańcuchów dostaw. Działania te muszą być wspomagane szerokim zakresem narzędzi doskonalenia struktur i procesów organizacyjnych. Przedsiębiorstwa w sektorze dóbr konsumpcyjnych częstego zakupu działają w otoczeniu nasilającej się konkurencji. Okoliczność ta powoduje, że generowana marża jest stosunkowo niska, co implikuje konieczność podejmowania działań obniżających koszty funkcjonowania tych przedsiębiorstw. Zarówno jednak instrumenty wspomagające działalność operacyjną, jak i zarządzanie w skali jednego przedsiębiorstwa nie umożliwiają takich osiągnięć, co wymaga poszukiwania nowych koncepcji działania. Chcąc sprostać wyzwaniom rynku,

przedsiębiorstwa muszą zwracać szczególną uwagę na otoczenie, w którym działają. Powiązania oraz poziom współpracy przedsiębiorstw z jego partnerami, zarówno z dostawcami, jak i z odbiorcami, stają się wykładnią sukcesu rynkowego. Faktem staje się konkurowanie całych łańcuchów dostaw (wszystkich ogniw od dostawcy surowców i komponentów produkcyjnych przez producentów, usługodawców logistycznych, jednostek rozliczeniowych do przedsiębiorstw handlowych, które uczestniczą w dostarczeniu danego produktu do ostatecznego klienta), a nie pojedynczych podmiotów. W tej sytuacji efektywny łańcuch dostaw staje się determinantą uzyskania przewagi konkurencyjnej.[1]

Fizyczna dystrybucja została rozwinięta w szerszą koncepcję zarządzania łańcuchem dostaw (SCM). Zarządzanie łańcuchem dostaw rozpoczyna się wcześniej niż fizyczna dystrybucja: wiąże się z zakupem właściwych czynników produkcji, wydajna ich zmianą w gotowe produkty oraz wysyłką do punktów przeznaczenia. Jeszcze szersza perspektywa to sprawdzanie, jak dostawcy producenta pozyskują swoje czynniki produkcji. Perspektywa łańcucha dostaw pomaga firmie zidentyfikować najlepszych dostawców i dystrybutorów i wesprzeć ich w podnoszeniu wydajności, co w ostatecznym wyniku zmniejsza koszty firmy.[2]

Koncepcja łańcucha dostaw ujmuje rynki jako punkty przeznaczenia i jest równoznaczna liniową koncepcją przepływu. W szerszej perspektywie firma postrzegana jest jako centrum sieci wartości, obejmującej dostawców firmy i dostawców jej dostawców oraz bezpośrednich klientów i ich końcowych klientów. W skład sieci wartości wchodzą związki z innymi osobami, takimi jak badacze, rządowe agencje zatwierdzające itp. Firma musi zgrać wszystkie te strony aby dostarczyć najlepszą wartość klientom na docelowym rynku. Powinna najpierw przemyśleć swój rynek docelowy i następnie, cofając się od punktu, budować swój łańcuch zaopatrzenia. Metoda ta nowi nazwę *planowania łańcucha popytu*. Logistyka rynkowa to planowanie infrastruktury pozwalającej zaspokoić popyt, a następnie umożliwiającej realizację i kontrolę fizycznego przepływu materiałów i towarów gotowych z miejsc wytworzenia do miejsc ich konsumpcji w celu przynoszącego zysk spełnienia wymagań klienta.[3]

Nowoczesne tendencje w logistyce przedsiębiorstw

Charakter zachodzących w przedsiębiorstwach procesów logistycznych jest ściśle powiązany z wszystkimi procesami zachodzącymi w przedsiębiorstwach, zarówno procesami materialnymi, takimi jak procesy produkcyjne, jak również z całą szeroko pojętą sferą regulacji (czyli de facto procesami zarządzania: zarówno w aspekcie strategicznym, jak i operacyjnym). Taki szeroki charakter

---

[1] Piekarska M., Mrozek-Kantak J., Lewandowska J. *Rozwiązania najważniejszych problemów współczesnych łańcuchów dostaw FMCG w Polsce,* Polski Kongres Logistyczny LOGISTICS 2006 pt: "Najlepsze praktyki w logistyce". Wydawnictwo Instytutu Logistyki i Magazynowania 2006.

[2] Kotler P., *Marketing*. Wydawnictwo Rebis. Poznań 2005, s. 76.

[3] Tamże, s. 560.

warunkuje konieczność właściwej koordynacji, konieczność nieustannego monitorowania relacji pomiędzy różnymi elementami systemu.

Rozpatrując procesy logistyczne z punktu widzenia przyjętego kryterium, czyli zapewnienia przez nie takiego skoordynowania w czasie i przestrzeni, które doprowadzi do dostępności produktów i usług dla klienta, istotny wpływ na ich kształt posiada strategia przedsiębiorstwa, uwzględniająca odpowiedź na pytanie o zakres procesów logistycznych realizowanych przez samo przedsiębiorstwo lub przez przedsiębiorstwa zewnętrzne, wynikająca z odpowiedzi na pytanie typu *make-or-buy* (wyprodukować czy kupić), które bezpośrednio wiążą się z istotą *outsourcingu*. Konieczność odpowiedzi na tak przedstawione pytanie ma bezpośredni wpływ na kształt całych procesów logistycznych zachodzących w łańcuchu logistycznym, jednak szczególnie silnie warunkuje ono kształt, szerokość i rodzaj działań logistycznych w sferze zaopatrzenia.

Wyjaśnić należy najpierw, czym charakteryzują się te dwa pojęcia. Obydwa odnoszą się do zakupu dóbr i usług niezbędnych do zrealizowania założonych procesów produkcyjnych w przedsiębiorstwie. Jak wskazuje analiza literatury przedmiotu[4] brak jest zgodności co do pojmowania tak wyróżnionych zagadnień, jako, że niektórzy autorzy przyjmują obydwa pojęcia za synonimy, inni z kolei rozróżniają je, uznając istotę *outsourcingu* jako podrzędną w stosunku do idei *make- or- buy*. Przyjąć należy, że podstawowa różnica pomiędzy wskazanymi koncepcjami odnosi się do ich zakresu, mianowicie *outsourcing* dotyczy usług wykonywanych dla przedsiębiorstwa, podczas gdy decyzje typu *make- or- buy* dotyczą również usług świadczonych w przedsiębiorstwie.

Decyzje typu wytworzyć lub kupić mają charakter strategiczny, jako że od nich zależy kształt wszystkich powiązań w łańcuchu logistycznym i de facto wielkość i rodzaje strumieni przepływu, jakie dają się zauważyć w łańcuchach. Mogą się odnosić przede wszystkim do dwóch typów decyzji: decyzji typu *make – or - buy* w zakresie zaopatrzenia w materiały i elementy kooperacyjne oraz decyzje w dziedzinie usług logistycznych.

W rozpatrywaniu problemu zakupić czy wytworzyć można wskazać na trzy podstawowe typy sytuacji[5]:

1. przedsiębiorstwo rozważa możliwość rezygnacji z produkcji już wykonywanej, na rzecz zakupu obecnie wytwarzanego danego materiału lub części,
2. przedsiębiorstwo posiada wolne moce produkcyjne, zatem rozważa możliwość samodzielnego podjęcia produkcji obecnie kupowanego materiału lub części,
3. przedsiębiorstwo nie posiada wolnych mocy produkcyjnych, jednak rozważa możliwość inwestycji w rozbudowę linii produkcyjnej , tak aby nie korzystać z zakupu danych komponentów u dostawców.

Oczywistą jest rzeczą, że każde z proponowanych rozwiązań posiada swoje

---

[4] J.Schafer-Kunz, C. Tewald, *Make or buy – Entscheidungen in der Logistik,* Deutscher Universitas Verlag Berlin, 1997, s.8, S. Krawczyk, *Logistyka w zarządzaniu marketingowym,* Wyd AE Wrocław 1998, s.137

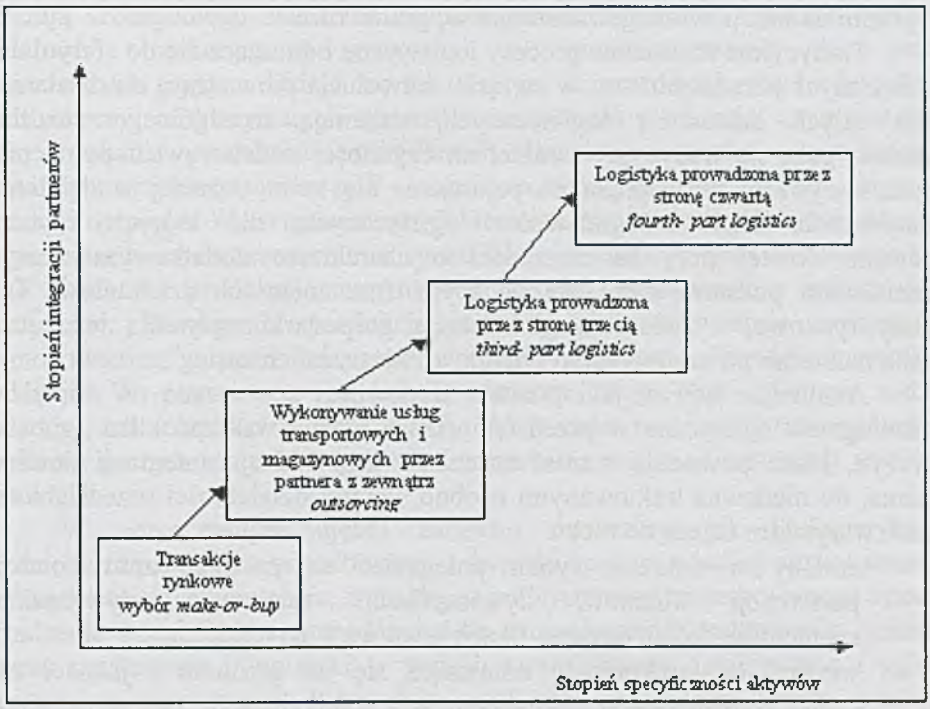
[5] S.Krawczyk, *Logistyka w zarządzaniu marketingiem,* Wyd. 3 zmienione, Wyd. AE we Wrocławiu, Wrocław 2000, s.165-166

wady i zalety, a decyzja dotycząca wskazanych rozwiązań ma charakter strategiczny dla przedsiębiorstwa. W sytuacji, gdy przedsiębiorstwo zdecyduje się wybrać produkcję (zasilanie) własne może zmniejszyć czas oczekiwania na produkt, ma możliwość elastycznego reagowania na zmiany popytu na rynku, a także ma możliwość lepszej kontroli jakości, jednak decyzja o produkcji wymaga zapewnienia odpowiednich warunków zarówno w zakresie sprzętu, jak również w zakresie odpowiednio wykwalifikowanej kadry. Wydaje się, że sensowniejszym może być skorzystanie z zaopatrzenia na rynku zewnętrznym, na którym istnieją wyspecjalizowane firmy produkujące poszukiwany przez przedsiębiorstwo komponent, poza tym ryzyko związane z wahaniami rynkowymi rozkłada się na dwóch partnerów: dostawcę i odbiorcę, a na dostawcy spoczywa odpowiedzialność za ewentualne braki jakościowe.

Problem dotyczący zakupu lub wytworzenia, ma szczególne znaczenie w odniesieniu do usług logistycznych. Wyraźnie daje się zauważyć tendencje wskazujące na coraz częstsze korzystanie w procesach logistycznych z usługodawców, zapewniających realizację działań ze sfery logistycznej, zarówno w zakresie transportu, jak również w zakresie magazynowania. Również w tym aspekcie można wyróżnić wyraźną ewolucję. Coraz częściej przedsiębiorstwa korzystają z usług przedsiębiorstw w jeszcze większym zakresie niż miało to miejsce do tej pory, często w pewien sposób konsolidując się z firmą – usługodawcą. W takim rozróżnieniu można zaobserwować podobieństwa pomiędzy systemem *make -or -buy*, a *outsourcingiem*. Wyróżnikiem *outsourcingu* jest fakt przekazywania różnorodnych funkcji przedsiębiorstwa, w tym wypadku logistycznych, dotyczących na przykład transportu i magazynowania do usługodawców zewnętrznych, przy czym przedsiębiorstwo delegujące zachowuje całkowitą kontrolę i planuje poszczególne działania. W takim ujęciu *outsourcing*, można uznać za etap późniejszy w ewolucji działań zachodzących pomiędzy nadawcą ładunków a przedsiębiorstwem usług logistycznych, natomiast cały pakiet działań ze sfery *make - or - buy* będzie etapem pierwotnym, w którym przedsiębiorstwo podejmuje decyzje o tym, które działania logistyczne prowadzi samodzielnie, a które będą przedmiotem zakupu. Przedstawione zagadnienia obrazuje rys. nr 1

Koncepcja *outsourcingu* pozwoliła na wyróżnienie w działalności przedsiębiorstw tzw. trzeciego (w najnowszych koncepcjach nawet czwartego) uczestnika procesów, czyli przedsiębiorstw, które świadczą usługi ze sfery logistycznej. Początkowo tak naprawdę usługi te dotyczyły tylko transportu i magazynowania, później jednak nabrały szerszego charakteru, tak jak to obrazuje przedstawiony schemat. Podjęcie decyzji o prowadzeniu działań logistycznych we własnym zakresie lub kupnie jej jako usługi zewnętrznej prowadzi do określenia zakresu *outsourcingu.* Wymieniony podział nie oddaje jednak w pełni zasadniczych obszarów działania. Dla *outsourcingu* wskazano tylko usługi związane z zamówieniami, przetwarzaniem danych czy doradztwem. Jednak można wskazać, iż jest możliwe, aby również usługi magazynowe lub transportowe były przedmiotem działań zewnętrznych pośredników. Natomiast możliwe jest także inne rozszerzenie koncepcji *make-or –buy,* gdyż na przykład przetwarzanie danych

można wskazać jako przedmiot tej koncepcji.



Rys.1. Ewolucja powiązań pomiędzy nadawcą zlecającym a usługodawcą logistycznym
Źródło: opracowanie własne na podstawie P.B. Schary, T.Skjott-Larsen, *Zarządzanie globalnym łańcuchem podaży,* Wyd. PWN Warszawa 2002, s.189,

Przedsiębiorstwa decydując się na zlecanie działań logistycznych na zewnątrz bardziej skupiają się na koordynacji działań w obszarze współpracy z usługodawcą, dzięki czemu mogą tak zorganizować swój system logistyczny, aby lepiej funkcjonował w łańcuchu. Wskazane rozwiązania z zakresu organizacji procesów logistycznych pozwalają na takie zbudowanie struktury, dzięki któremu możliwe będzie wykorzystanie wszystkich atutów opisanych rozwiązań. Należałoby się jednak zastanowić, czy przedsiębiorstwa są w stanie w taki sposób dokonać budowy łańcuchów logistycznych, aby wszelkie działania logistyczne i procesy związane z ich koordynowaniem przebiegały w sposób umożliwiający zbudowanie struktury wydolnej, dostosowanej do potrzeb, tak, aby możliwe było zrealizowanie założonego celu organizacji zarządzanej logistycznie, czyli dotarcie do odpowiedniego klienta i zapewnienie mu dostępności oferowanych dóbr. Z punktu widzenia przedsiębiorstwa wspomniane procesy powinny być efektywne zarówno pod względem organizacyjnym, jak i ekonomicznym.

Wyraźnie obserwowalne we współczesnej gospodarce procesy wskazują na ewolucję, prowadzącą do sytuacji, w której klasyczne podziały wyodrębniające na rynku zakłady produkcyjne, handlowe i usługowe wyraźnie się zacierają. Coraz częściej zamiast o systemach logistycznych wyodrębnionych firm mówimy o

systemach logistycznych całych łańcuchów logistycznych. Zatem definiowanie istoty czynności i działań logistycznych staje się coraz trudniejsze, przede wszystkim na fakt powolnego zacierania się granic firm.

Tradycyjnie rozumiane procesy logistyczne odnoszące się do sfery działań wewnętrznych przedsiębiorstw, w związku z ewolucją prowadzącą do działania na rynku całych łańcuchów logistycznych, nabierają szczególnego znaczenia. Wyraźnie gubi się tradycyjny podział na czynności podstawowe i pomocnicze, przede wszystkim ze względu na pojawienie się strony trzeciej w działaniach logistycznych, czyli usługodawców logistycznych, dla których czynności uznawane do tej pory za czynności o charakterze dodatkowym stają się czynnościami podstawowymi, stanowiącymi fundament ich działalności. Także zmiany rynkowe, a zwłaszcza globalizacja gospodarki wpływają w znaczący sposób na kształt procesów logistycznych, a zwłaszcza ich zasięg[6].

Analizując wpływ jaki posiada środowisko zewnętrzne na zarządzanie marketingowo-logistyczne w przedsiębiorstwie można wskazać kilka zjawisk i przyczyn, które powodują wzrost znaczenia tego rodzaju integracji pomiędzy dwiema, do niedawna traktowanymi osobno sferami działalności przedsiębiorstw. Przede wszystkim należą do nich[7]:

- zmiany w zakresie rynku polegające na zróżnicowaniu potrzeb i preferencji klientów, dywersyfikacji towarów, indywidualizacji segmentów rynku, dywersyfikacji towarów i innych;
- wzrastającą konkurencję odnoszącą się do poziomu i jakości usług świadczonych na rzecz klientów, wynikających ze wzrastających wymagań w zakresie użyteczności i dodatkowych korzyści jakich oczekują oni w trakcie zakupu;
- skrócenie cyklu życia produktów;
- zmiany w zakresie handlu, a zwłaszcza jego koncentracja, wpływająca na powstanie nowych kanałów zbytu;
- chęć wykorzystywania przez przedsiębiorstwa w zakresie zarządzania efektu synergii, który odnosi się zarówno do sfery makro- jak i mikroekonomicznej;
- rozwój nowych technologii w zakresie logistyki dystrybucji, jak również w sferze promocji, sprzedaży itp.;
- integracja i globalizacja rynków, a także,
- wzrost przedsiębiorczości na rynku i innowacyjności w zakresie działalności gospodarczej i rynkowej.

Wszystkie wymienione czynniki prowadzą do sytuacji, w której przedsiębiorstwa chcąc osiągnąć sukces rynkowy muszą uwzględniać w swojej strategii działania obie te sfery równocześnie. W tym zakresie widać wyraźnie, że przyjęta strategia marketingowa powinna szczególnie mocno akcentować elementy

---

[6] Kot S.: *Analysing the Effectiveness of Supply Chain Management Through Customer Satisfaction Assessment - Dairy Industry Case.* [in:] Problemy povysenija effektivnosti dejatel'nosti predprijatij. Pod red. A.I.Rubachova. Brest.gosud.techn.univ. Brest 2005, s.97-100 ISBN 985-493-012-2

[7] P. Blaik, *Logistyka,* PWE Warszawa 2001, s.218

z zakresu logistyki, gdyż w dobie obecnego globalnego rynku problemy logistyki, wynikające z konieczności dotarcia do coraz dalej położonych rynków zbytu nabierają szczególnego znaczenia. Bardzo istotne znaczenie z punktu widzenia działalności marketingowo-logistycznej w przedsiębiorstwie ma proces prognozowania popytu. Dzieje się tak dlatego, iż przedsiębiorstwa odchodzą w chwili obecnej od klasycznych systemów zarządzania produkcją, czyli systemów *push* - pchania produktów przez kanały logistyczne zanim popyt zostanie zgłoszony, na rzecz systemów *pull* – ciągnięcia, w których produkt jest „ciągnięty" w reakcji na popyt. W związku z tym faktem istnieje konieczność szczegółowego prognozowania zapotrzebowania na rynku tak, aby możliwe było dostosowanie do niego wielkości produkcji i wymaganej do jej zrealizowania infrastruktury logistycznej. Planowanie produkcji jest, więc konsekwentnie związane z prognozowaniem popytu, który tak naprawdę wymusza odpowiednią wielkość produkcji. W planowaniu produkcji pomocne mogą być różnego rodzaju procedury, na przykład system MRP, który daje możliwość szczegółowego określenia potrzeb materiałowych niezbędnych do realizacji założonej wielkości produkcji[8].

W nowoczesnym ujęciu zarówno marketing, jak i logistykę w przedsiębiorstwie można potraktować w dwojaki sposób, z jednej strony stanowią one współistniejące koncepcje, z drugiej są podsystemami zintegrowanego systemu zarządzania przedsiębiorstwem. Powoduje to konieczność traktowania działań z zakresu marketingu i logistyki w sposób kompleksowy, jako istotne i główne orientacje w zarządzaniu, które dają możliwość osiągnięcia trwałej przewagi rynkowej, oraz podniesienia wartości dla klienta. Przedstawione zależności ilustruje rys. 2.

W przedstawionym podejściu wyraźnie widoczne jest traktowanie marketingu i logistyki jako z jednej strony odrębnych, a z drugiej komplementarnych dziedzin działalności przedsiębiorstwa. Jest to podejście ze wszech miar słuszne, gdyż tylko w taki sposób istnieje możliwość osiągnięcia efektu synergii w przedsiębiorstwie w zakresie zarządzania marketingowo-logistycznego.

Właściwe zorganizowanie sfery zarządzania marketingowo-logistycznego wymaga od przedsiębiorstwa właściwego ustalenia i skoordynowania celów każdej ze sfer, w taki sposób aby uwzględniając odrębność każdej z nich i wypracować wspólną, zintegrowaną strategię marketingowo-logistyczną.

[8] S. Krawczyk, *Zarządzanie procesami logistycznymi*, PWE Warszawa 2001, s.61

Rys. 2. Dualność postrzegania marketingu i logistyki w przedsiębiorstwie
Źródło: opracowanie własne na podstawie: Integracja marketingu i logistyki – wybrane problemy, pod red. R. Matwiejczuka, Politechnika Opolska, Opole 2005, s. 56

Podsumowaniem rozważań o wzajemnej komplementarności działań z zakresu marketingu i logistyki w przedsiębiorstwie może być uzupełnienie znanej, zaproponowanej przez R. Lauterborna[9] formuły „4C" klienta. Obejmuje ona następujące elementy: potrzeby i pragnienia klienta (*Customer needs and wants*), koszt dla klienta (*Cost to the customer*), wygoda zakupu (*Convenience*) i dostarczanie informacji (*Communication).* Zostają one uzupełnione znaną, nazywaną popularnie „definicją logistyki dla laików" formułą „7W": właściwy stan i struktura produktu, właściwa informacja, właściwa ilość, właściwa jakość, właściwy czas, właściwe miejsce, właściwy koszt realizacji zleceń. Takie podejście, akcentujące specyficzne perspektywy i efekty integracji marketingu i logistyki w strategii konkurencji, uwzględniające zarówno kosztowe, jak i rynkowe konsekwencje, stanowią właściwą podstawę do osiągnięcia korzystnej - w sensie długofalowym pozycji przedsiębiorstwa na rynku.

Literatura

1. Blaik P.: *Logistyka,* PWE Warszawa 2001
2. *Integracja marketingu i logistyki – wybrane problemy,* pod red. R. Matwiejczuka, Politechnika Opolska, Opole 2005

[9] Cyt. za: PH. Kotler, *Marketing. Analiza, planowanie, wdrażanie i kontrola,* Gebtthner i S-ka, Warszawa 1994, s. 91

3. Kot S.: *Analysing the Effectiveness of Supply Chain Management Through Customer Satisfaction Assessment - Dairy Industry Case.* [in:] Problemy povysenija effektivnosti dejatel'nosti predprijatij. Pod red. A.I.Rubachova. Brest.gosud.techn.univ. Brest 2005, s.97-100 ISBN 985-493-012-2
4. Kotler P.: *Marketing.* Wydawnictwo Rebis. Poznań 2005
5. Kotler P.: *Marketing. Analiza, planowanie, wdrażanie i kontrola,* Gebtthner i S-ka, Warszawa 1994
6. Krawczyk S.: *Logistyka w zarządzaniu marketingiem,* Wyd. 3 zmienione, Wyd. AE we Wrocławiu, Wrocław 2000
7. Krawczyk S.: *Zarządzanie procesami logistycznymi,* PWE Warszawa 2001
8. Piekarska M., Mrozek-Kantak J., Lewandowska J.: *Rozwiązania najważniejszych problemów współczesnych łańcuchów dostaw FMCG w Polsce,* Polski Kongres Logistyczny LOGISTICS 2006 pt: "Najlepsze praktyki w logistyce". Wydawnictwo Instytutu Logistyki i Magazynowania 2006
9. Schafer-Kunz J.: C.Tewald, *Make or buy – Entscheidungen in der Logistik,* Deutscher Universitas Verlag Berlin, 1997
10. Schary P.B., T.Skjott-Larsen: *Zarządzanie globalnym łańcuchem podaży,* Wyd. PWN Warszawa 2002

ROZDZIAŁ XI

SYSTEM NEW WPI+

Mirosław SIEMION

Każda jednostka musi nieustannie analizować i identyfikować warunki, które mogłyby w sposób istotny wpływać na jej zdolność do realizacji celów. Proces ten dokonywany jest przez systemy informatyczne, które zdobywają, przetwarzają i przekazują informację o zdarzeniach, działaniach i warunkach wskazujących na zmiany, na które jednostka musi reagować. Odpowiednie informacje obejmują dane branżowe, gospodarcze i prawne otrzymywane ze źródeł zewnętrznych oraz generowane wewnętrznie, na przykład o zmianach w preferencjach klientów, nowej technologii wpływającej na procesy produkcyjne przedsiębiorstwa, działaniach konkurentów, zmianach w prawie. Proces identyfikacji i reakcji na zmieniające się warunki może zostać zaprogramowany i wprowadzony w odpowiedni system informatyczny przedsiębiorstwa.

Spośród wielu systemów informatycznych na szczególną uwagę zasługuje opracowany przez Bytomską Spółkę Informatyczną COIG – 4 Sp. z.o.o. z siedzibą w Bytomiu nowy **System newWPI+** obejmujący moduły:

- Studium Wykonalności – Modele Finansowe
- Wspomaganie Procesu Inwestycji
- Rozliczenie Funduszy Unijnych
- Struktura Organizacyjna
- Zarządzanie Obiektami Inwentarzowymi
- Centralna Kartoteka Przetargów
- Centralna Kartoteka Umów

System został opracowany jako narzędzie dające możliwość monitorowania przebiegu procesu realizacji zadań w skali makro- i mikroekonomicznej w dowolnej jego fazie, rozliczenia zadań pod względem finansowym i wykonanym zakresem rzeczowym.

Szczególny nacisk położono na dostosowanie systemu do zasad monitorowania i rozliczania inwestycji prowadzonych w ramach Funduszy Unijnych.

Funkcje prezentowanego systemu ułatwiają rozliczanie środków finansowych przeznaczonych na realizację zadań, na bieżąco monitorują wykorzystanie zasobów finansowych takich jak: środki własne, zaciągnięte kredyty, otrzymane dotacje (z różnych Programów Pomocowych, Strukturalnych, Operacyjnych), itp.

System newWPI+ stwarza podstawy kontroli przebiegu realizacji planu, usprawnia i ułatwia rozliczanie zakończonych zadań, w tym w jednostkach wielozakładowych,

Celem Systemu nweWPI jest unowocześnieniem sposobu zarządzania

projektami/zadaniami w przedsiębiorstwie. System ma z jednej strony zagwarantować długofalowe bezpieczeństwo funkcjonowania infrastruktury w przedsiębiorstwie, z drugiej natomiast stanowić będzie podstawowe narzędzie wspomagające podejmowanie decyzji w zakresie realizacji projektów/zadań za każdym szczeblu zarządzania.

Rozbudowana klasyfikacja i parametryzacja systemu pozwala prowadzić szczegółowy monitoring realizacji zadań.

Moduły systemu

Studium Wykonalności – Modele Finansowe

Moduł w głównej mierze przeznaczony to tworzenia analiz opłacalności inwestycji, obliczania składników ekonomicznych, budowania planów technicznych, strategicznych, operacyjnych. Zawiera w pełni definiowaną przez użytkownika sekcję budowania modelu finansowego – dowolne pozycje w formie „drzewiastej", wzory matematycznej, wariantowość (na przykład: wariant optymistyczny, wariant pesymistyczny). Uzyskane wyniki możliwe do podziału: rok, kwartał, miesiąc, dzień.

Wspomaganie Procesu Inwestycji

Ewidencjonowanie, monitorowanie i rozliczenie inwestycji.

Rozliczanie Funduszy Unijnych

Ewidencjonowanie, monitorowanie i rozliczenie inwestycji prowadzonych w ramach Funduszy Unijnych.

Rozliczanie Awarii i Remontów

Ewidencjonowanie, monitorowanie i rozliczenie awarii, serwisu i remontów.

Struktura Organizacyjna

Moduł przeznaczony do zarządzania strukturą organizacyjną firmy. Dwa rodzaje struktury:

- organizacyjna komórki organizacyjne
- technologiczna – miejsca pracy

Zarządzanie Obiektami Inwentarzowymi

Zarządzanie majątkiem

Centralna Kartoteka Przetargów

Zarządzanie centralną kartoteką przetargów

Centralna Kartoteka Umów

W strukturach wielozakładowych możliwości prowadzenia umów na

szczeblu Zarządu – przyznanie części budżetu umowy o wykorzystania dla poszczególnych zakładów wchodzących w skład struktury organizacyjnej Firmy.

Strategiczne cele systemu

Wdrożenie Systemu nweWPI ma zapewnić spełnienie następujących celów:

- Integrację informacji pochodzących z różnych obszarów funkcjonowania firmy w jednolitym środowisku – współpraca z modułami zintegrowanymi systemu informatycznego w zakresie:
  1. Systemu Finansowo – Księgowego
  2. Systemu Gospodarki Materiałowej
  3. Systemu Środków Trwałych
  4. Systemu Zamówień
  5. Centralnego Rejestru Umów
  6. Centralnego Rejestru Przetargów
  7. Centralnej Kartoteki Kontrahentów
  8. Struktury Organizacyjnej
- Sprawowanie kontroli nad realizowanymi projektami
- Zarządzanie zadaniami
- Analizę sytuacji finansowe i rzeczowej prowadzonych zadań
- Optymalne gospodarowanie dysponowanymi zasobami – budżetem
- Integracja informacji i ich udostępnienie upoważnionym osobom zgodnie z planem praw dostępu
- W przypadku struktury wielozakładowej:
  1. Standaryzacja komputerowej ewidencji realizacji zadań we wszystkich jednostkach
  2. centralny monitoring i zarządzanie
  3. standaryzacja analiz i raportowania
  4. możliwość konsolidacji raportów i sprawozdań
  5. tworzenie sprawozdań zbiorczych z wybranej jednostki lub wszystkich jednostek łącznie
- Przyspieszenie dostępu do wszystkich zadań źródłowych jak i wynikowych
- Dostęp do danych archiwalnych z okresów poprzednich
- Możliwość przeglądania informacji zapisanych w systemie w wielowymiarowych przekrojach
- Przeprowadzanie bieżących analiz poprzez zastosowanie kryteriów wyboru wybranych zadań
- Automatyzację rutynowych, powtarzalnych czynności
- Ukierunkowanie na:
  1. Monitoring finansowy lub rzeczowy
  2. Sprawozdawczość lokalną lub nadrzędną

Cechy systemu

Podstawowe cechy Systemu newWPI$^+$ to:

Zgodność z prawem

1. Rozporządzenie Ministra Rozwoju Regionalnego z dnia 27 kwietnia 2007 w sprawie trybu kontroli realizacji projektów i programów współfinansowanych ze środków Funduszy Strukturalnych i Funduszy Spójności, Dz. U. Nr 90 poz.602;
2. Ustawa z dnia 29 września 1994 o rachunkowości, Dz. U. 1994 nr 121 poz. 591;
3. Ustawa z dnia 7 lipca 1994 r. Prawo budowlane, Dz. U. Nr 207 poz.2016 z 2003 roku z późniejszymi zmianami;
4. Rozporządzenie Rady Ministrów z dnia 13 lipca 2000r. dot. Klasyfikacji projektu wg Nomenklatury Jednostek Terytorialnych dla Celów Statystycznych w Polsce i innych krajach U.E.;
5. Ustawa z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych.

Gwarantuje zgodność z aktualnie obowiązującym prawem. Zespół projektantów i programistów zajmujący się rozwojem systemu na bieżąco śledzi zmiany w ustawodawstwie oraz dokonuje właściwych modyfikacji systemu.

Modułowość

Oznacza, że każdy moduł dziedzinowy realizuje funkcje tematyczne, powiązane hierarchicznie. Budowa taka umożliwia konfigurowanie systemu w zależności od wymagań użytkownika.

Pełna integracja

Zapewnia integrację elementów systemu względem siebie bez względu na konfigurację (wzajemne przenikanie danych). System newWPI$^+$ umożliwia wprowadzenie jednokrotnie danych źródłowych (w ramach modułu) z możliwością korzystania z nich w innych modułach, biorąc pod uwagę prawa dostępu do nich.

Dane

Zaletą systemu jest:

- Ujednolicenie wprowadzenia danych w każdej jednostce (w strukturze wielozakładowej) wg tych samych kryteriów,
- Zastosowanie (w strukturze wielozakładowej) centralnych kartotek,
- Informacja jest tylko raz wprowadzana do systemu,
- Gromadzone dane są na poziomie elementarnym, brak wyników pośrednich,
- Ułatwienie wprowadzania poprzez zastosowanie katalogów (dane powtarzające się są przechowywane w katalogach do wielokrotnego wykorzystania)

Tak trzymane elementarne dane w bazie danych, umożliwiają tworzenie

sprawozdań i analiz za dowolny okres czasu wstecz (odwzorowanie stanu realizacji zadania w czasie przeszłym).

Poufność danych

Realizowana poprzez rozbudowany mechanizm kontroli uprawnień i rejestracji działań użytkowników. Przy eksporcie danych na zewnątrz możliwe jest automatyczne zabezpieczenie pliku hasłem.

Bezpieczeństwo danych

Realizowane poprzez mechanizmy zapewniające pełne bezpieczeństwo oraz poufność danych zawartych we wszystkich dostępnych modułach.
Możliwa jest wielopoziomowa ochrona wprowadzanych danych:

- Standardowe administracyjne mechanizmy ochrony dostępu do bazy danych oraz systemu operacyjnego przez osoby nieuprawnione,
- Rejestrowanie użytkowników,
- Hasło dostępu,
- Mechanizm autoryzacji użytkowników otwierających sesje systemowe. Istnieje możliwość zastosowania narzędzi autoryzacji firm zewnętrznych, które można dostosować do używania w ramach systemu,
- Mechanizm autoryzacji użytkowników do systemu do wykonywania czynności oraz dostępu do tabel systemowych,
- Kontrola użytkowników zarejestrowanych w systemie,
- Mechanizm kontroli uprawnień w poszczególnych obszarach działania,
- Przypisanie funkcji użytkownikowi w ramach systemu,
- Rejestracje zdarzeń z informacją kiedy i kto wykonywał funkcję, dokonał zmieny, wyemitował raport lub zestawienie,
- Algorytmy kodujące dane przesyłane pomiędzy serwerami danych a użytkownikami lub urządzeniami zewnętrznymi – narzędzia firm zewnętrznych.

Różnorodność baz danych

Pozwala na pracę w technologii relacyjnej bazy danych:
INFORMIX, MS SQL SERWER, Postgre SQL

Skalowana ilość użytkowników

Pozwala na pracę dowolnej ilości użytkowników systemu bez konieczności przekonfigurowania Systemu oraz bez wpływu na efektywność pracy.

Centralny system z rozproszonym dostępem

Oznacza, że dane przechowywane są w jednej spójnej bazie danych, a dostęp do nich możliwy jest z dowolnego miejsca. System newWPI^{+} to system wielodostępny, tzn. korzystać z niego może wielu użytkowników równocześnie i niezależnie od siebie.

Skalowalność

Oznacza, że w zależności od potrzeb istnieje możliwość dowolnego umiejscowienia serwerów:

- Centrum Przetwarzania Danych – DATA CENTER,
- Serwer w jednostce centralnej (wszystkie stacje robocze podpięte do serwera centralnego),
- Serwer w jednostce regionalnej (stacje robocze rozmieszczone w jednostkach podległych),
- Serwer w jednostce podległej

Integracja z systemami zewnętrznymi

Wyniki działania raportów emitowanych w systemie mogą być zapisane jako dokument TXT, XLS. Pozwala to wysyłać dane do MS Word, MS Excel. Możliwa jest integracja z innymi systemami funkcjonującymi w jednostce organizacyjnej (jedno- lub dwu- kierunkowa).

System newWPI^{+} zasadniczo implementowany jest jako całość, jednak możliwe jest użytkowanie poszczególnych modułów dziedzinowych jako niezależne całości lub współpracujące z oprogramowaniem innych producentów poprzez interfejsy komunikacyjne.

Ciągły nadzór autorski projektantów i programistów nad systemem, optymalizacja rozwiązań oraz ciągły proces śledzenia nowych rozwiązań w dziedzinie informatyki są gwarancją na stałe udoskonalanie systemu i wzbogacanie go o nowe techniki.

Wymiana danych pomiędzy systemami

System newWPI^{+} może współpracować z: Systemem Finansowo-Księgowym, Systemem Gospodarki Materiałowej, Systemem Środków Trwałych oraz Systemem Zamówień już funkcjonującym w firmie.

Opracowano na podstawie danych udostępnionych przez Bytomską Spółkę Informatyczną COIG – 4 Sp. z o.o. z siedzibą w Bytomiu.

CZĘŚĆ

PROBLEMY BEZPIECZEŃSTWA

ROZDZIAŁ XII

ZARZĄDZANIE RYZYKIEM PROJEKTOWYM

Franciszek WOŁOWSKI

Wprowadzenie

Na ostatnim z naszych spotkań w Szczyrku zostały przedstawione zasady zarządzania ryzykiem w systemach informacyjnych czyli tych już eksploatowanych bądź przewidzianych do eksploatacji. W tym artykule przedstawione zostały zasady zarządzania ryzykiem projektowym.

Zarządzanie ryzykiem w procesie projektowania systemów IT różni się w zasadniczy sposób od podejścia do zarządzania ryzykiem samych systemów. Wprawdzie samo ryzyko oblicza się bądź szacuje się według tych samych wzorów i metod lecz podczas gdy ryzyko dla systemów informacyjnych jest zjawiskiem jedynie negatywnym to w projektowaniu systemów ryzyko może mieć zarówno negatywną wartość (opóźnienie, wzrost kosztów) jak i pozytywną (przyspieszenie, obniżka kosztów). Ponieważ w języku polskim ryzyko jest raczej postrzegane jako coś negatywnego to pozytywne ryzyko związane z przedsięwzięciami zmierzającymi do osiągnięcia lepszych wyników w procesie projektowania częściej nazywane jest więc możliwością natomiast pozytywnym odpowiednikiem zagrożenia jest szansa. W artykule dla uproszczenia najczęściej używane jest pojęcie ryzyka obejmujące również możliwości. Również sam sposób zarządzania ryzykiem projektowym znacznie różni się od zarządzania ryzykiem systemów eksploatowanych, w których to stosując różnego rodzaju zabezpieczenia staramy się obniżyć ryzyko zniszczenia bądź uszkodzenia zasobów, braku dostępności tych zasobów lub utraty dobrego imienia organizacji. Natomiast zarządzając ryzykiem projektowym stosujemy różnego rodzaju środki zaradcze dla uniknięcia negatywnych zjawisk ale również środki które mogą pozytywnie wpłynąć na wykonanie celu jakim jest wytworzenie systemu informacyjnego.

Szef projektu zarządzając pracami projektowymi w procesie zarządzenia ryzyka podsumowuje zagrożenia i syanse, jakie dostrzega dla określonego projektu, w czasie jego konstruowania, po czym są one aktualizowane przy każdym przeglądzie.

W wielu projektach o małym ryzyku wystarcza przygotować jedynie opis tekstowy spostrzeganego ryzyka, jednak w trudnych, rozciągniętych w czasie projektach o dużej wartości komitet sterujący może żądać bardziej formalnej oceny ryzyka.. Taki właśnie pełny i formalny sposób zarządzania ryzykiem zostanie przedstawiony w tym opracowaniu.

Kryteria sukcesu projektu.

Projekt można określić jako tymczasowy wysiłek, którego celem jest dostarczenie unikalnego produktu lub grupy produktów potrzebnych do przyszłego świadczenia unikalnej usługi. Opierając się na tej definicji można określić następujące charakterystyki projektu: zakres, czas, zasoby, ryzyko. charakterystyki te stanowią podstawę definicji kryteriów sukcesu projektu. Należy więc .te kryteria bliżej zdefiniować aby móc określić zagrożenia i szanse i w konsekwencji ryzyka i możliwości związane z projektem.

Zakres projektu określa „pracę, którą należy wykonać w celu dostarczenia produktu o określonych cechach i określonej funkcjonalności"

Zakres w ujęciu produktowym można opisać funkcją, której argumentami są dostarczane produkty i ich jakość. Im więcej produktów ma być dostarczanych, tym więcej pracy należy włożyć w ich wykonanie lub tym większe środki należy przeznaczyć na ich zakup. Analogicznie, im wyższa ma być jakość produktu, tym więcej pracy wymaga jego wytworzenie.

ZAKRES = Z_1 (PRODUKTY, JAKOŚĆ)

Zakres w ujęciu procesowym jest funkcją, której argumentami są dostępne zasoby i czas. *ZAKRES = Z_2 (CZAS, ZASOBY)* W większości przypadków wraz ze wzrostem zaangażowanych zasobów maleje czas wykonywania zadań. Należy jednak pamiętać, że nie zawsze tak jest. Na przykład, rozbudowa zespołu może spowodować w początkowym okresie spadek jego efektywności

Czas. Zadania określone w projekcie muszą być wykonane w ściśle określonym czasie. Czas ten wyznacza się na podstawie: dostępności zasobów oraz zapotrzebowania na produkt. Jeżeli produkt nie zostanie dostarczony w wymaganym czasie, zapotrzebowanie zostanie zaspokojone przez innego wykonawcę

Zasoby można określić następującym wzorem: *ZASOBY = WYKONAWCA + ODBIORCA + BUDŻET*

Ryzyko Ponieważ celem projektu jest wytworzenie unikalnego produktu, ustalenia dokonane w trakcie planowania nie są precyzyjne a nawet niektóre istotne parametry mogą nie zostać zidentyfikowane w fazie definiowania projektu. Ryzyko można więc określić funkcją: RYZYKO = R (ZAKRES, CZAS, ZASOBY) .Niestety ryzyko w projektach informatycznych jest bardzo wysokie – ogromna większość dużych projektów kończy się z naruszeniem ustalonych na początku kryteriów lub całkowitym fiaskiem.

Zamieszczona powyżej definicja kryteriów sukcesu projektu sugeruje jedynie negatywny aspekt ryzyka. Kierownik projektu uwzględniający jedynie ten aspekt będzie dążyć do jego zminimalizowania. Istnieje więc niebezpieczeństwo zaprzepaszczenia nowych szans, które pojawią się w czasie wykonywania projektu i które stworzą nowe możliwości. W dobie rosnącej konkurencji takie podejście może być niekorzystne dla organizacji. Znacznie bardziej obiecujące wydaje się podejście aktywne. Jego istotną cechą jest dążenie do wykorzystywania nadarzających się okazji, nawet jeżeli wiąże się to z pewnym ryzykiem. W podejściu tym uwzględnia się pozytywny aspekt ryzyka – możliwości, a kryteria

sukcesu projektu definiuje się jako osiągnięcie maksymalnego zysku przy zakładanym poziomie ryzyka.

Procesy Zarządzania Ryzykiem Projektowym

Najczęściej zarządzanie projektem określa się jako stosowanie wiedzy, zdolności, narzędzi i technik w czasie wykonywania operacji i działań projektowych w celu spełnienia lub przekroczenia oczekiwań stron zainteresowanych pomyślnym zakończeniem projektu (Duncan: 1996).

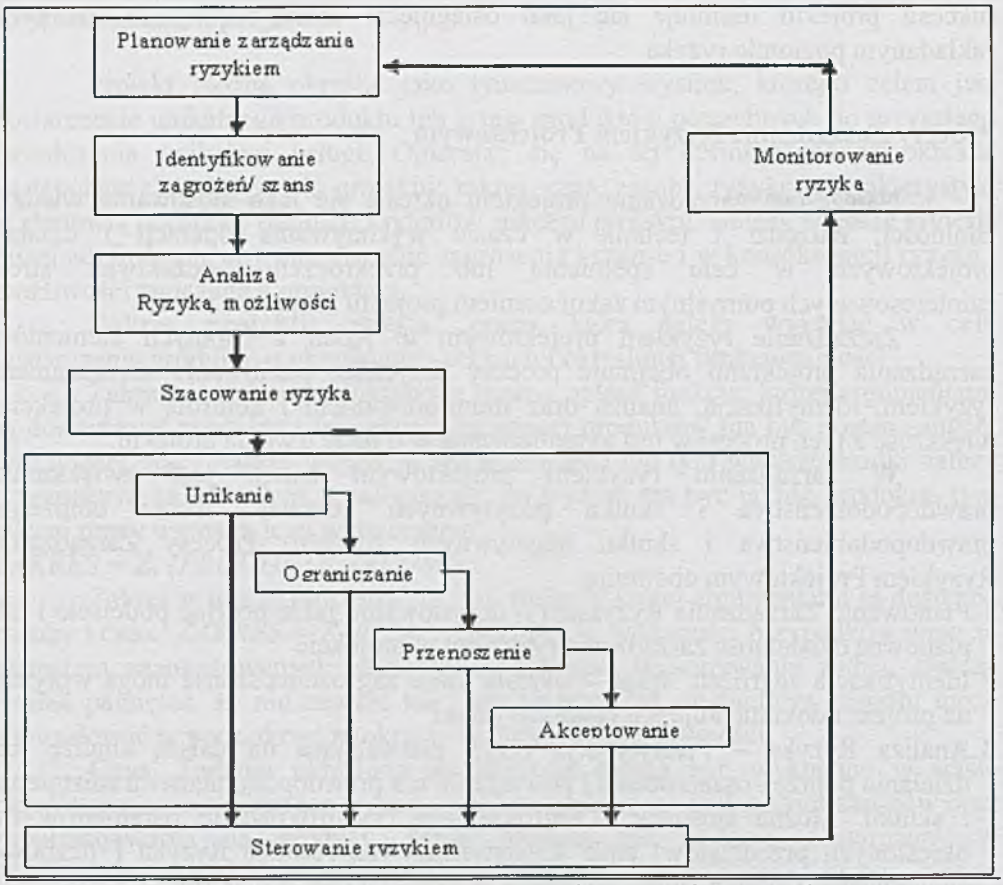
Zarządzanie ryzykiem projektowym to jeden z istotnych elementów zarządzania projektami obejmuje procesy dotyczące planowania zarządzaniem ryzykiem, identyfikacją, analizą oraz monitorowaniem i kontrolą w projekcie, większość z tych procesów jest aktualizowana w trakcie trwania projektu.

W zarządzaniu ryzykiem projektowym celem jest zwiększenie prawdopodobieństwa i skutku pozytywnych zdarzeń oraz obniżenie prawdopodobieństwa i skutku negatywnych zdarzeń. Procesy Zarządzania Ryzykiem Projektowym obejmują:

1. Planowanie Zarządzania Ryzykiem – decydowanie jakie przyjąć podejście i jak planować działalność zarządzania ryzykiem w projekcie
2. Identyfikacja zagrożeń/ szans – określa które zagrożenia/szanse mogą wpłynąć na projekt i dokumentuje ich charakterystyki
3. Analiza Ryzyka – Priorytyzacja ryzyk pozwalająca na dalszą analizę lub działania poprzez oszacowanie i powiązanie ich prawdopodobieństwa zaistnienia i skutku. Można stosować Kwalifikatywną (kwalifikowanie parametrów do określonych przedziałów) bądź Kwantyfikatywną Analizę Ryzyka (liczbowe analizowanie wpływu zidentyfikowanych ryzyk na cele projektowe).
4. Planowanie reakcji na ryzyko – opracowywanie procedur i technik w celu poprawy możliwości i redukcji zagrożeń na cele projektowe
5. Sterowanie – śledzenie zidentyfikowanych ryzyk,
6. Monitorowanie ryzyka monitorowanie ryzyk szczątkowych, identyfikowanie nowych ryzyk, wykonywanie planów łagodzenia ryzyk i ocena efektywności tych działań podczas cyklu życia projektu.

Procesy te wzajemnie oddziaływają na siebie jak również na inne procesy z innych obszarów wiedzy. Każdy proces dotyczy wysiłków od jednej do wielu osób lub grup osób w zależności od potrzeb projektu. Każdy z procesów zdarza się co najmniej raz w każdym projekcie i zdarza się w jednej lub więcej fazach, jeśli projekt jest podzielony na fazy.

Ryzyko projektowe jest nie pewnym zdarzeniem lub okolicznością, która jeśli się urzeczywistni, wywiera pozytywny lub negatywny skutek na cele projektowe takie jak czas, koszt, zakres lub jakość (tj gdy cel czasowy projektu jest dany zgodnie z uzgodnionym harmonogramem; gdy cel kosztu projektu jest zadany w ramach uzgodnionego kosztu itd.). Ryzyko ma jedną lub wiele przyczyn- i jeśli się urzeczywistni- wywołuje jeden lub wiele skutków.



Rys. 1. *Relacje między etapami zarządzania ryzykiem projektu*
Źródło: opracowanie własne na podstawie (*Project Risk Management Procedures*: 2003)

Na przykład przyczyną może być wymaganie uzyskania środowiskowego (oficjalnego) zezwolenia na rozpoczęcie pracy lub narzucone ograniczenia zatrudnienia (przypisania) personelu do projektu. Zdarzenie jest ryzykownym dlatego, że uzyskanie z instytucji udzielającej pozwolenia może zająć więcej czasu niż zaplanowano lub personel może nie być odpowiedni dla tej pracy. Jeśli któreś z tych niepewnych zdarzeń się urzeczywistni, wpłynie to na koszty projektu, harmonogram lub wykonanie. Warunki ryzyka mogą obejmować aspekty środowiska projektowego lub organizacji, które mogą przyczyniać się do ryzyka projektowego takiego jak kiepskie praktyki zarządzania projektem, brak zintegrowanego systemu zarządzania, wiele jednoczesnych projektów lub zależność od zewnętrznych uczestników, którzy nie podlegają kontroli.

Ryzyko projektowe ma swoje źródło w niepewności, że jest obecne we wszystkich projektach. Ryzyka rozpoznane to te, które zostały zidentyfikowane i przeanalizowane oraz w odniesieniu do których jest możliwe przeprowadzenie procesu planowania dla tych ryzyk wg metod przyjętych w danej organizacji. Ryzykiem nieznanym nie da się zarządzać zapobiegawczo a rozważną reakcją

zespołu projektowego przeciwko takiemu ryzyku może być zastosowanie ogólnych rozwiązań, takich jakie stosuje się przeciwko wszystkim znanym ryzykom, dla których nie znaleziono rozwiązań efektywnych kosztowo lub możliwości stworzenia zapobiegawczej reakcji.

Organizacje postrzegają ryzyko jako ich relację do zagrożeń sukcesu projektu lub możliwości powiększenia szans sukcesu projektowego. Ryzyka, które zagrażają projektowi mogą być akceptowane jeśli są one w równowadze z korzyściami, które można uzyskać przez utrzymywanie tego ryzyka na założonym poziomie. Na przykład, przyjęcie szybkiej ścieżki harmonogramu, który może być opanowany, jest ryzykiem podjętym aby uzyskać wcześniejszy termin ukończenia. Ryzyka, które są możliwościami, takie jak przyspieszenie pracy, które mogą być osiągnięte przez dołączenie dodatkowego personelu, mogą być realizowane aby zyskać na celach projektowych.

Osoby i organizacje muszą podchodzić do ryzyka tak aby wpływać zarówno na precyzję postrzegania ryzyka jak i na sposób reakcji na nie. Podejście do ryzyka powinny być wykonane jasno tak jak to tylko możliwe. Konsekwentnym podejściem do ryzyka, które spełnia wymagania organizacji, powinno być wypracowanie dla każdego projektu spójnego podejścia do ryzyka a informowanie o ryzykach i sposobach obchodzenie się z nimi powinno być otwarte i uczciwe. Reakcja na ryzyko odzwierciedla organizacyjne postrzeganie równowagi pomiędzy podejmowaniem ryzyka i unikaniem ryzyka.

Aby osiągnąć sukces, organizacja musi być zaangażowana w kierowaniu zarządzaniem ryzykiem w całym projekcie. Jednym z objawów zaangażowania organizacji w projekcie jest jej poświęcenie przy gromadzeniu danych o wysokiej jakości o ryzykach projektowych i jego charakterystykach.

Planowanie Zarządzania Ryzykiem Projektowym

Współczesne zarządzanie projektami wymaga, aby procesy zarządzania projektem były ściśle zintegrowane z procesami zarządzania ryzykiem. W zależności od wielkości projektu i własnych doświadczeń, organizacje mogą wypracować różne rozwiązania tego problemu.

Staranne i jasne planowanie zwiększa możliwość sukcesu pozostałych procesów zarządzania ryzykiem. Planowanie zarządzania ryzykiem jest procesem decydowania jak rozpocząć i prowadzić działalność zarządzania ryzykiem w projekcie. Planowanie procesów zarządzania ryzykiem jest ważne aby zapewnić żeby poziom, typ i widoczność zarządzania ryzykiem były współmierne do zarówno ryzyka jak i ważności projektu dla organizacji aby zapewnić dostateczne środki i czas dla czynności zarządzania ryzykiem oraz ustalić i uzgodnić podstawy szacowania ryzyka. Proces Planowania Zarządzaniem Ryzykiem powinien być wykonany, przed planowaniem projektu, gdyż jest to kluczowe dla pomyślnego wykonania pozostałych procesów.

Dokumentem uzyskanym w wyniku procesu planowania jest „Plan zarządzania ryzykiem"

Plan zarządzania ryzykiem opisuje jak zarządzanie ryzykiem będzie skonstruowane i wykonywane w projekcie. Staje się on podzbiorem planu zarządzania projektem.

Plan zarządzania ryzykiem obejmuje co następuje:

Metodologia. Definiuje podejścia, narzędzia i dane źródłowe, które mogą być używane do zarządzania ryzykiem w projekcie.

Role i odpowiedzialności. Określają przywództwo, wspomaganie i członków zespołu zarządzania ryzykiem dla wszystkich typów działalności w planie zarządzania ryzykiem, przypisanie ludzi do tych ról i uściślenie ich odpowiedzialności.

Budżetowanie. Przypisanie zasobów i oszacowanie kosztów niezbędnych do zarządzania ryzykiem dla włączenia do podstawowych kosztów projektu.

Wyznaczanie terminów. Określa kiedy i jak często będzie wykonywany proces zarządzania ryzykiem w trakcie cyklu życia projektu i ustala czynności zarządzania ryzykiem do włączenia do harmonogramu projektu.

Kategorie ryzyk. Dostarcza struktur, które zapewniają pełny proces systematycznego identyfikowania ryzyk z spójnym poziomem szczegółowości i przyczyniają się do efektywności i jakości Identyfikacji Ryzyk. Kategorie ryzyka mogą być korygowane w procesie Identyfikowania Ryzyk.

Definicje prawdopodobieństwa i skutku / wpływu urzeczywistnienia się ryzyk. Jakość i wiarygodność procesu Analizy Ryzyka wymaga aby zostały zdefiniowane różne poziomy prawdopodobieństwa ryzyk i ich skutków. Ogólne definicje poziomów prawdopodobieństwa i poziomów skutków są dopasowywane do indywidualnych projektów podczas procesu Planowania Zarządzaniem Ryzykiem przy stosowaniu procesu Analizy Ryzyka.

Może być tu używana odpowiednia skala reprezentująca wartości prawdopodobieństwa od „bardzo mało prawdopodobnego" do „prawie pewnego". Alternatywnie, mogą być używane przypisywane numeryczne prawdopodobieństwo w skali ogólnej (np. 0.1, 0.3, 0.5, 0.7, 0.9). Skala skutków odzwierciedla znaczenie skutku, bądź negatywnego dla zagrożeń bądź pozytywnego dla szans. Skale skutku są specyficzne dla celów potencjalnych ataków, typu i rozmiaru projektu, strategii organizacji i stanu finansowego oraz wrażliwości organizacji na określony atak. Kwalifikatywne skale skutków są prostymi uporządkowanymi opisami takimi jak „bardzo niski", „niski", „średni", wysoki, i „bardzo wysoki", odzwierciedlający coraz mocniejszy wpływ jaki został określony przez organizację. Alternatywnie, przypisane są numeryczne skale wartości do tych skutków. Te wartości mogą być liniowe (np. 0.1, 0.3, 0.5, 0.7, 0.9) lub nie liniowe (np.0.05, 0.1, 0.2, 0.4, 0.8).

Poniższa tabela jest przykładem definicji negatywnego skutku, jakie mogą być używane przy oszacowaniu skutku ryzyka na cele projektowe. Ta tabela ilustruje zarówno kwalifikatywne jak i kwantyfiatywne podejścia. Cyfry nie mają zamiaru sugerować, że kwalifikatywne i kwantyfiatywne oznaczenia są ekwiwalentne lecz pokazać dwie alternatywy w jednej tablicy.

Opis uwarunkowań dla skal skutków wystąpienia ryzyk dla głównych celów projektowych (Wyszczególnienie obejmuje jedynie warunki dla skutków negatywnych)					
Cele projektowe	Skale względne lub numeryczne				
	Bardzo niskie/.05	Niskie/.010	Srednie/ .20	Wysokie / .40	Bardzo wysokie /.80
Koszt	Nieznaczny wzrost kosztów	<10%wzrost kosztów	10-20% wzrost kosztów	wzrost kosztów o 20-40%	wzrost kosztów >40%
Czas	Nieznaczny wzrost czasu	5%wzrost czasu	5-10% wzrost czasu	10-20% wzrost czasu	>20% wzrost czasu trwania projektu
Zakres	Ledwie zauważalne zmniejszenie zakresu	Dotknięte mniej istotne obszary zakresu	Dotknięte Istotne obszary zakresu	Nieakceptowalne dla sponsorów zmniejszenie zakresu	Końcowy produkt projektu jest praktycznie bezużyteczny
Jakość	Ledwie zauważalne zmniejszenie jakości	Dotknięte tylko bardzo wymagające zastosowania	Obniżenie jakości wymaga zatwierdzenia przez sponsora	Obniżenie jakości jest nieakceptowalne dla sponsorów	Końcowy produkt projektu jest praktycznie niezdatny do użytku

Tablica ta przedstawia przykłady definicji skutków dla czterech różnych celów projektowych. Dla konkretnego projektu i dla organizacyjnych progów ryzyka definicje te powinny być dopasowane w procesie Planowania Zarządzania Ryzykiem. Definicje skutków dla szans mogą być opracowane w podobny sposób.

- **Macierz prawdopodobieństwa i skutku.** Ryzyka są uszeregowane zgodnie z ich potencjalnymi implikacjami na spełnienie celów projektowych.
- **Skorygowane tolerancje udziałowców (interesariuszy).**
- **Formaty raportowania.**
- **Obserwacja /Śledzenie.** Określenie w jaki sposób będzie się dokumentować wszystkie aspekty ryzykownych działań aby dane te można było wykorzystać w bieżącym projekcie oraz w przyszłych projektach w postaci zestawu potrzeb i nauczek. Określenie czy i w jaki sposób procesy zarządzania ryzykiem będą audytowane.

Identyfikacja Zagrożeń

Celem identyfikowania zagrożeń jest określenie czynników niepewności projektu (zagrożeń i szans). Właściwe wykonanie tego zadania wymaga dogłębnej znajomości organizacji wykonujących projekt, wykorzystywanych rozwiązań technologicznych, uwarunkowań rynkowych (kulturowych, ekonomicznych, prawnych) oraz biznesowych celów projektów.

Identyfikacja Ryzyka określa, które ryzyka i możliwości mogą wpływać na projekt i dokumentuje ich charakterystyki.

Identyfikacja zagrożeń jest procesem interaktywnym ponieważ nowe zagrożenia mogą zostać rozpoznane w trakcie progresu w cyklu życia projektu. Częstotliwość iteracji i kto ma być uczestnikiem w każdym cyklu będzie się zmieniać od przypadku do przypadku. Proces Identyfikacji zagrożeń zwykle prowadzi do procesu Analizy Ryzyka.

Rezultaty z Identyfikacji zagrożeń zamieszcza się w dokumencie zwanym

rejestrem zagrożeń/ ryzyk (częściej zwany jest rejestrem ryzyk). Pierwsze zapisy do rejestru ryzyk, pochodzą z planu zarządzania projektem. Stopniowo rejestr ryzyka uzupełniany jest wynikami z innych procesów zarządzania ryzykiem. W rejestrze pojawiają się następujące informacje: Lista zidentyfikowanych zagrożeń, Lista potencjalnych reakcji na ryzyko. Źródła przyczyn ryzyka.

Analiza Ryzyka

- Analiza Ryzyka obejmuje metody priorytyzacji zidentyfikowanych ryzyk dla przyszłych działań, takich jak Planowanie Reakcji na Ryzyko. Organizacje mogą poprawić efektywność osiągów projektowych przez skupienie się na ryzykach o wysokim priorytecie. Analiza Ryzyka szacuje priorytety zidentyfikowanych ryzyk używając ich prawdopodobieństwa urzeczywistnienia się, odpowiadających im skutków na cele projektowe jeśli te ryzyka wystąpią, jak również inne czynniki takie jak ramy czasowe i tolerancja ryzyka projektowych ograniczeń kosztów, harmonogramu, zakresu i jakości.
- Definicje poziomów prawdopodobieństwa i wpływu i wywiadów ekspertów, mogą pomóc skorygować stronniczości, które często objawiają się w używanych w tym procesie danch. Krytyczny czas czynności związanych z ryzykiem może wyolbrzymiać znaczenie ryzyka. Ocena jakości dostępnej w projekcie informacji również pomaga zrozumieć oszacowanie ważności ryzyka w projekcie.
- Kwalifikatywna Analiza Ryzyka jest zwykle szybka i kosztowo efektywna, oznacza to ustalenie priorytetów dla Planowania Reakcji na Ryzyko i położyć podwaliny pod Kwantyfikatywną Analizę Ryzyka, jeśli takowa jest potrzebna. Kwalifikatywna Analiza Ryzyka powinna być rewidowana w trakcie projektowego cyklu życia aby uaktualnić wywołane przez zmiany ryzyka projektowe. Kwalifikatywna Analiza Ryzyka wymaga wyjść dla procesów Planowania Zarządzania Ryzykiem i Identyfikacji Ryzyk. Ten proces może prowadzić do Kwantyfikatywnej Analizy Ryzyka lub bezpośrednio do Planowania Reakcji na Ryzyko.

Szacowanie prawdopodobieństwa i skutku ryzyka

Oszacowanie prawdopodobieństwa ryzyka bada możliwość zaistnienia każdego z ryzyk, które może się urzeczywistnić. Oszacowanie skutku ryzyka bada potencjalny wpływ na cele projektu takie jak czas, koszt, zakres lub jakość włączając zarówno wpływ negatywny dla zagrożeń i pozytywny dla sprzyjających okoliczności

Prawdopodobieństwo i skutek są szacowane dla każdego zidentyfikowanego ryzyka. Ryzyko może być szacowane podczas wywiadu lub spotkań z uczestnikami wybranymi z uwagi na ich znajomość kategorii ryzyk tego programu. Włączeni są również członkowie zespołu projektowego i być może osoby o odpowiedniej wiedzy z zewnątrz projektu. Wymagana jest opinia eksperta, gdy organizacja posiada niewielką ilość informacji w swojej bazie danych z

poprzednich projektów. Doświadczony doradca może kierować dyskusją gdy uczestnicy mają niewielkie doświadczenie w szacowaniu ryzyka.

Poziom prawdopodobieństwa i dla każdego z ryzyk i wpływu na każdy z celów jest oceniany podczas wywiadu lub spotkania. Rejestrowane są również szczegóły wyjaśniające, włączając w to uzasadnienie szacunku przypisanych poziomów. Prawdopodobieństwo i skutek ryzyka są oceniane zgodnie z definicjami podanymi w planie zarządzania ryzykiem. Czasami, ryzyka z jednoznacznie niskimi poziomami prawdopodobieństwa i skutku nie będą oceniane, lecz będą włączane do list obserwowanych dla przyszłego monitorowania.

Macierz prawdopodobieństwa i skutku

Ryzyko może zostać uszeregowane według poziomów ryzyk i reakcji na ryzyko. Poziomy są przypisywane w oparciu o szacunki prawdopodobieństwa i skutków tych ryzyk. Ocena istotności ryzyk i w związku z tym, priorytetu zajmowania się nimi jest zwykle prowadzona stosując tablice lub macierze prawdopodobieństwa i skutku. Tego typu macierze specyfikują kombinacje prawdopodobieństwa i skutku co prowadzi do oceny ryzyk o priorytetach niskim, średnim lub wysokim. Mogą być używane terminy przymiotnikowe lub wartości numeryczne w zależności od preferencji organizacji.

Organizacja powinna określić które kombinacje prawdopodobieństwa i skutku powodują zaklasyfikowanie do wysokiego ryzyka (ciemny obszar szarości z najwyższymi wartościami liczbowymi), średniego ryzyka (obszar średniej szarości z pośrednimi wartościami liczbowymi) i niskiego ryzyka (obszar jasno szary z najniższymi wartościami liczbowymi). Zwykle te zasady klasyfikacji ryzyk są określane przez organizację przed projektem i włączają je do swoich aktywów procesów organizacyjnych (Karta projektu).W procesie planowania zarządzania ryzykiem można dostosowywać zasady klasyfikacji ryzyk do specyfiki danego projektu.

Przedstawiona na poniższym rysunku macierz jest jedynie przykładem

Macierz Prawdopodobieństwa i Skutku

Prawdo podobieństwo	Zagrożenia					Szanse/ sprzyjające okoliczności				
0,90	0,05	0,09	0,18	0,36	0,72	0,72	0,36	0,18	0,09	0,05
0,70	0,04	0,07	0,14	0,28	0,56	0,56	0,28	0,14	0,07	0,04
0,50	0,03	0,05	0,10	0,20	0,40	0,40	0,20	0,10	0,05	0,03
0,30	0,02	0,03	0,06	0,12	0,24	0,24	0,12	0,06	0,03	0,02
0,10	0,01	0,01	0,02	0,04	0,08	0,08	0,04	0,02	0,01	0,01
Wpływ →	0,05	0,10	0,20	0,40	0,80	0,80	0,40	0,20	0,10	0,05

Wpływ (współczynnik skali) na cele (np. koszt, czas, zakres lub jakość)
Ryzyko = Prawdopodobieństwo x Wpływ
Każde ryzyko jest ustalane na podstawie prawdopodobieństwa wystąpienia zdarzenia i skutku/ wpływu na cele jeśli miał miejsce. W macierzy zakreślono progi organizacyjne dla niskiego, średniego lub wysokiego ryzyka i określono czy ryzyko dla tego celu jest notowane jako wysokie (ciemny obszar szarości), średnie(obszar średniej szarości) czy niskie(obszar jasno szary)

Jak widać na rysunku organizacja może klasyfikować ryzyka oddzielnie względem każdego z celów (np. :kosztu, czasu i zagrożeń) Ponadto, może również opracować sposoby określania ogólnej klasyfikacji poszczególnych ryzyk. Wreszcie, w jednej macierzy można ująć sposoby klasyfikacji szans i zagrożeń, posługując się definicjami różnych poziomów skutków, właściwych dla każdej z tych grup ryzyk.

Klasyfikacja ryzyk ułatwia reakcje na poszczególne ryzyka. Na przykład, ryzyka mające w razie wystąpienia negatywny wpływ na cele projektowe (zagrożenia) i znajdujące się w strefie wysokiej istotności (ciemnoszarej-czerwonej) mogą wymagać priorytetowego działania i zdecydowanej strategii reagowania.. Natomiast w wypadku zagrożeń znajdujących się w strefie niskiej istotności (jasnej szarości) działania zapobiegawcze mogą ograniczyć się do umieszczenia tych zagrożeń na liście obserwowanych ryzyk lub uwzględnienia ich w rezerwie na nieprzewidziane okoliczności (rezerwy projektowej).
Podobną logiką można kierować się w przypadku szans. Te które znalazły się w strefie wysokiej częstotliwości (ciemnoszarej), ponieważ są najłatwiejsze do podjęcia i oferują największe korzyści, powinny być najszybciej objęte działaniami. W wypadku szans o niskiej korzyści (jasno szarej, wystarczy ograniczyć się do monitorowania.

Ocena jakości danych o ryzykach

Warunkiem wiarygodności kwalifikatywnej analizy ryzyka jest użycie dokładnych i obiektywnych danych. Analiza jakości danych o ryzykach jest techniką oceny stopnia przydatności tych danych w zarządzaniu ryzykiem. Obejmuje ona sprawdzenie zakresu, w jakim pozwalają one zrozumieć same ryzyka a także dokładności, poprawności, wiarygodności i spójności danych o ryzykach.

Korzystanie z danych o niskiej jakości może prowadzić do niewielkiej użyteczności dla projektu rezultatów kwalifikatywnej analizy ryzyka. Jeśli jakość danych okaże się niemożliwa do zaakceptowania, może zaistnieć potrzeba zebrania lepszych danych. Gromadzenie informacji o ryzykach jest często trudne i absorbuje czas i zasoby większe aniżeli pierwotnie planowano.

Kategoryzacja ryzyk

Ryzyka projektu można podzielić na kategorie według źródeł ryzyk (np. za pomocą struktury podziału ryzyk), obszarów projektu, których dotyczą ryzyka lub według innych użytecznych kryteriów (na przykład etapów projektu). Pozwala to określić obszary w projekcie, które są najbardziej narażone na wpływ niepewności. Grupowanie ryzyk według wspólnych przyczyn źródłowych może prowadzić do określenia skutecznych reakcji na ryzyko.

Ocena pilności ryzyk

W pierwszej kolejności można się zająć ryzykami, które wymagają reakcji w bliskim terminie. Wskaźnikami takiej priorytetowości ryzyk mogą być : czas potrzebny, by reakcja na ryzyko odniosła skutek, symptomy oraz znaki ostrzegawcze a także klasyfikacja ryzyk.

Rezultaty analizy ryzyka.

Rezultaty analizy ryzyka aktualizują Rejestr ryzyk. Informacje dodane w trakcie kwalifikatywnej analizy ryzyka obejmują:

- **lista ryzyk projektu uporządkowanych według istotności.** Można opracować oddzielne listy najważniejszych ryzyk z punktu widzenia kosztu, czasu, zakresu i jakości, ponieważ organizacje mogą przedkładać jeden z tych celów nad inne.
- **Ryzyka pogrupowane według kategorii**. Kategoryzacja ryzyk może ujawnić wspólne przyczyny źródłowe ryzyk lub obszary projektu wymagające szczególnej uwagi. Wykrycie obszarów koncentracji ryzyka może zwiększyć skuteczność reakcji na ryzyka.
- **Lista ryzyk wymagających reakcji w bliskim terminie.** Można utworzyć odrębną grupę ryzyk wymagających pilnej reakcji i tych którymi można się zająć nieco później.
- **Lista ryzyk wymagających dodatkowej analizy i reakcji**. W przypadku niektórych ryzyk uzasadnione jest przeprowadzenie dalszej analizy, w tym kwantyfikatywnej analizy ryzyka a także określonych reakcji.
- **Listy obserwowanych ryzyk o niskiej istotności.**

Planowanie reakcji na ryzyko

Celem planowania reakcji na ryzyko jest

a) zwiększenie prawdopodobieństwa sukcesu poprzez ograniczenie prawdopodobieństwa i/lub skutków ryzyka o wysokim prawdopodobieństwie,
b) zidentyfikowanie i określenie najbardziej krytycznych kategorii ryzyka, składników kosztów i elementów harmonogramu,
c) zapewnienie wybiegającego w przyszłość planu mającego na celu ograniczenie ryzyka i zawierającego opis działań, odpowiedzialności oraz daty.

Reakcje planuje się na podstawie wyników analizy ryzyka. Mogą mieć one wiele form w zależności w strategii i kultury organizacji.

W większości przypadków można je zaliczyć do jednej z następujących kategorii:

a) unikanie,
b) akceptowanie,
c) ograniczanie,
d) przenoszenie.

Unikanie ryzyka polega na zaplanowaniu prac lub wyborze rozwiązań w

taki sposób, żeby całkowicie wyeliminować ryzyko. Działania te zwykle sprowadzają się do ograniczenia zakresu projektu (zrezygnowania z najbardziej ryzykownych zadań) lub wyboru alternatywnych rozwiązań (np. innej wersji oprogramowania lub produktu innego wykonawcy). w szczególności zgodnie z tą strategią pracy systemu nie wolno podejmować ryzyka, które przekracza ustalony dopuszczalny poziom,

Idea zarządzania ryzykiem wymaga by ta metoda była obecna **w każdym rekomendowanym wariancie realizacji celów** wprost lub poprzez ogólne założenie przyjęte z góry dla całego systemu.

Uniknięcie ryzyka jest możliwe tylko w specyficznych warunkach.

Akceptacja/ Retencja (zatrzymanie) ryzyka oznacza:

- stworzenie specjalnego, wewnętrznego funduszu na pokrycie szkód lub innego, własnego zabezpieczenia w wypadku zaistnienia szkody (aktywna retencja)
- oczekiwanie na szkodę bez tworzenia szczególnego systemu zabezpieczenia przy możliwości jej pokrycia z bieżących, wolnych zasobów (pasywna retencja).

Akceptacja/ Retencja nie powinna być stosowana dla ryzyk, które nie spełniają wszystkich z niżej wymienionych warunków:

- łatwe do przewidzenia skutki i wysokość potencjalnej szkody,
- relatywnie niska wysokość pojedynczej szkody,
- małe prawdopodobieństwo znacznej kumulacji szkód.

Ograniczenie ryzyka. Efekt ten można uzyskać na dwa sposoby. Pierwszy polega na analizie przyczyn ryzyka i podejmowaniu z odpowiednim wyprzedzeniem działań ograniczających prawdopodobieństwo ich wystąpienia (podejście aktywne). Drugi na reagowaniu na zaistniałe zdarzenia w celu zminimalizowania ich negatywnych skutków (podejście reaktywne).

Należy sobie zdawać sprawę, że ograniczanie ryzyka poniżej pewnego poziomu nie jest opłacalne. W pewnym momencie ponoszone koszty zaczną przekraczać potencjalne zyski. Dlatego należy ustalić ryzyko dopuszczalne, które zależy od stosowanej polityki organizacji i ograniczania ryzyka doprowadzać do tego poziomu.

Jeżeli ryzyka nie można uniknąć, ani ograniczyć, ani zaakceptować należy podjąć próbę jego **przeniesienia na inny podmiot**. Działanie to polega na przekazaniu wykonania wybranego zadania i zarządzania związanym z nim ryzykiem podwykonawcy, którego doświadczenie lub zasoby dają rękojmię skutecznego rozwiązania problemu. Przykładem takiego przeniesienia może być outsourcing i ubezpieczenie. Dla zagrożeń związanych z siłami natury są to też najczęściej jedyne możliwe metody transferu Należy pamiętać, że przeniesienie ryzyka na inny podmiot nie eliminuje go całkowicie. Umożliwia jednak zastąpienie go innym, łatwiejszym w zarządzaniu. Na przykład, jeżeli organizacja będąca głównym wykonawcą projektu nie dysponuje zasobami pozwalającymi odpowiednio szybko przeszkolić pracowników odbiorcy, może wykonanie tego zadania powierzyć firmie szkoleniowej. W ten sposób ryzyko niedotrzymania terminu zostaje przeniesione na podwykonawcę.

Sterowanie ryzykiem

Sterowanie ryzykiem obejmuje dwa rodzaje działań. Działania pierwszego rodzaju często określa się jako wprowadzanie korekt. Ich istotą jest wdrażanie planów reakcji opracowanych we wcześniejszej fazie zarządzania ryzykiem. Sygnałem do ich rozpoczęcia są określone, wyspecyfikowane w planach reakcji, wyniki procesów monitorowania ryzyka.

Działania drugiego rodzaju polegają na inicjowaniu procesów ponownego identyfikowania ryzyka projektu ,ich szacowania oraz planowania reakcji. Działania te, w zależności od polityki zarządzania ryzykiem, podejmuje się:

a) w ustalonych odstępach czasu (np. raz w miesiącu),
b) po osiągnięciu określonych punktów węzłowych projektu (milestones),
c) po zaobserwowaniu istotnych zmian w otoczeniu projektu (np. po zmianie uwarunkowań prawnych),
d) po uzyskaniu dodatkowej wiedzy wskazującej na dezaktualizację obowiązujących oszacowań ryzyka lub planów reakcji (np. dotyczącej błędów w stosowanym oprogramowaniu).

Monitorowanie ryzyka

Ryzyko związane z wykonywaniem poszczególnych zadań zależy w projekcie od wielu czynników takich, jak:

- zmiany w otoczeniu projektu,
- stopień wykonania pozostałych zadań projektu,
- procesy i interakcje w zespole projektowym.

W zależności od ich oddziaływania ryzyko może rosnąć lub maleć wraz z upływem czasu zmuszając kierownika projektu do podjęcia odpowiednich działań. Ważne jest, aby działania te zostały podjęte we właściwym momencie. Zbyt częste, zwykle przedwczesne, reakcje mogą dezorganizować pracę zespołu i powodować nieuzasadniony wzrost kosztów projektu. Natomiast, zbyt późne wdrożenie planów reakcji może znacząco ograniczyć ich skuteczność. Dlatego ryzyko projektu powinno być stale monitorowanie tak, aby kierownik projektu dysponował aktualnymi informacjami i mógł, na ich podstawie, uruchomić odpowiednie procesy sterujące.

W większości projektów informatycznych najistotniejszym źródłem ryzyka są członkowie zespołu projektowego. W takich przypadkach monitorowanie ryzyka polega głównie na monitorowaniu wykonywanych prac wykonywanych przez poszczególne osoby i ciągłym weryfikowaniu związanych z nimi oszacowań ryzyka. Poniżej przedstawiono najczęściej stosowane techniki:

- **zebrania pracowników**
- **raporty indywidualne**
- **indywidualne spotkania** .

Monitorowanie prac zespołu zazwyczaj wpływa pozytywnie na jakość i efektywność pracy. Należy również pamiętać, że w praktyce stosowanie tylko

jednej z wymienionych wyżej metod bardzo rzadko przynosi pozytywne rezultaty. Zwykle należy je łączyć.

Literatura

1. *Project Risk Management Procedures* (2003), White Paper, Canadian Risk Technologies Inc.,
2. *A Guide to the Project Management Body of Knowledge Third Edition (PMBOK® Guide)*
3. *Project Management Handbook* (1999), California Department of Transportation, 1999
4. Duncan W.R. (1996), *A Guide To The Project Management Body of Knowledge,* PMI Standards Committee, PA 19073-3299 USA, 1996

ROZDZIAŁ XIII

BEZPIECZEŃSTWO INFORMACJI – PODEJŚCIE HOLISTYCZNE

Andrzej BIAŁAS

1. Wprowadzenie

W ostatnim okresie spotyka się często termin „holistyczny" wykorzystywany w odniesieniu do bezpieczeństwa informacji, na przykład:

- holistyczny pogląd na temat bezpieczeństwa przedsiębiorstwa, rozumiany jako uwzględnienie nie tylko zabezpieczeń IT, ale i innych typów zabezpieczeń, dobieranych na podstawie analizy ryzyka (wykorzystano metodę Octave, uwagę skupiono na platformie Microsoft) [1];
- bezpieczeństwo holistyczne, rozumiane jako integracja bezpieczeństwa informacji i bezpieczeństwa fizycznego [2];
- bezpieczeństwo holistyczne, rozumiane jako integracja procesów zarządzania bezpieczeństwem informacji z procesami biznesowymi przy założeniu, że mogą być one realizowane z wykorzystaniem usług IT [3];
- bezpieczeństwo holistyczne, rozumiane jako wielowątkowe podejście do osiągnięcia zgodności instytucji finansowej z amerykańską ustawą GLBA (Gramm-Leach-Bliley Act), obowiązującą dla usług finansowych [4];
- bezpieczeństwo holistyczne, rozumiane jako siedmiowarstwowy system ochrony (ochrona fizyczna ośrodka przetwarzania danych, bezpieczeństwo sieci, hostów, oprogramowania systemowego, aplikacji, bezpieczeństwo osobowe, audyt) [5];
- konieczność wielowarstwowej ochrony zasobów instytucji, gdyż zabezpieczenia wówczas wzajemnie się uzupełniają [6].

Na wstępie należałoby się odnieść do samego pojęcia „holistyczny". Według [7] termin ten, stosowany w teorii i metodologii nauk społecznych, przyjmuje, że „twierdzenia dotyczące złożonych zjawisk społecznych niedostępnych obserwacji nie dadzą się sprowadzić do wypowiedzi o zachowaniach jednostek i ich grup" i głosi, że „prawidłowości zjawisk społecznych nie dają się wywnioskować z prawidłowości ich składników". Termin pochodzi od holizmu (*ang. holism z gr. hólos 'cały'*), czyli teorii filozoficznej sformułowanej po raz pierwszy przez polityka południowoafrykańskiego Jana Christiaana Smutsa (1870-1950), głoszącej, że determinującymi czynnikami w naturze są "całości", których nie da się sprowadzić do sumy ich części. Holizm (od *gr. holos* – całość) to pogląd, według którego wszelkie zjawiska tworzą układy całościowe, podlegające swoistym prawidłowościom, których nie można

wywnioskować na podstawie wiedzy o prawidłowościach rządzących ich składnikami. Całości nie da się sprowadzić do sumy jej składników.

Niniejsza publikacja nawiązuje do wykładu autora, wygłoszonego na sesji „Bezpieczeństwo holistyczne: ochrona zasobów, cyberśledztwo oraz zapewnienie ciągłości działania" w ramach XXIII Jesiennych Spotkań Polskiego Towarzystwa Informatycznego, które odbyły sie w dniach 16-18 października 2007 w Wiśle. Opracowanie porusza różne aspekty holistycznego, czyli całościowego, kompleksowego podejścia do rozwiązywania problemów bezpieczeństwa informacji.

2. Interdyscyplinarny charakter zagadnienia bezpieczeństwa informacji

Problemy bezpieczeństwa informacji mają charakter interdyscyplinarny i wymagają uwzględnienia zagadnień z wielu różnych dziedzin. Analizując problemy bezpieczeństwa widziane przez pryzmat zagrożeń spotyka się nie tylko zagadnienia teleinformatyczne, lecz również organizacyjne, dotyczące personelu i otoczenia fizycznego. Rozpatrując nawet najprostsze systemy można zetknąć się z takimi problemami, jak na przykład:

- zbiory danych można nielegalnie skopiować lub sfałszować;
- urządzenia do przetwarzania danych są podatne na wyłączenia lub zakłócenia zasilania;
- oprogramowanie może posiadać nieznane błędy zniekształcające wyniki przetwarzania lub boczne wejścia, może być zawirusowane, a nawet nielegalne;
- zabezpieczenia wbudowane do sprzętu lub oprogramowania mogą być źle skonfigurowane, mogą być omijane lub po prostu nieskuteczne;
- administrator systemu może popełniać błędy podczas konfigurowania systemów, może być niewłaściwie przeszkolony lub nielojalny i ujawnić wiedzę o zabezpieczeniach;
- programista systemowy może pomyłkowo lub celowo zneutralizować zabezpieczenia, dopisać swoje tajne wejścia czy wprowadzić znaczące podatności na ataki zewnętrzne;
- użytkownicy na ogół stwarzają najwięcej problemów, takich jak: nadużycia w zakresie identyfikacji i uwierzytelnienia, ujawnianie haseł, subtelne modyfikacje oprogramowania, zawirusowanie, oszustwa czy niedbalstwo;
- personel serwisujący, zwłaszcza pracujący bez nadzoru i korzystający ze specjalistycznych narzędzi, może przechwycić informacje, wyłączyć zabezpieczenia, doprowadzić do awarii, zmienić konfigurację lub wprowadzić trudne do wykrycia podatności;
- należy również liczyć się ze szpiegostwem, zwłaszcza ze strony nieuczciwej konkurencji;
- należy pamiętać, że systemy teleinformatyczne jako wytwory techniki mają określoną niezawodność oraz pracują w określonym środowisku

fizycznym, do którego odnoszą się zagrożenia, typu włamanie, pożar czy zalanie.

Środki i metody do rozwiązywania tych problemów powinny uwzględniać tę różnorodność. Praktyka pokazuje, że dany problem może być najefektywniej rozwiązany przez zaaplikowanie, na podstawie wyników analizy ryzyka, grupy różnorodnych zabezpieczeń oddziaływujących na zagrożenia i podatności wielokierunkowo, wspierających się wzajemnie i stanowiących pewną całość. Taka strategia działania wyraża istotę określenia „podejście holistyczne do bezpieczeństwa informacji". Jako przykłady takich działań można podać następujące przypadki:

- nie wystarczy zakupić drogie, certyfikowane urządzenia szyfrujące, skoro informacja nie jest właściwie klasyfikowana i oznaczana, nie opracowano zasad zarządzania kluczami kryptograficznymi, archiwizacji, nie zapewniono właściwej ochrony fizycznej i nie przeszkolono personelu;
- zakup kosztownego systemu zaporowego nie ochroni zasobów informacyjnych instytucji, jeśli nie zostanie wprowadzona kontrola nośników wymiennych i procedury dostępu.

Podejście holistyczne do bezpieczeństwa informacji ułatwia ciągłą adaptację systemu bezpieczeństwa do zmian zachodzących w procesach biznesowych, w systemach teleinformatycznych wykorzystywanych do ich realizacji i w środowisku zagrożeń. Poza tym ułatwia identyfikację nowych zagrożeń, podatności oraz złożonych relacji zachodzących w instytucji i jej systemie bezpieczeństwa.

3. Holistyczne, probiznesowe podejście do zarządzania bezpieczeństwem informacji w instytucji

Holistyczne podejście do zagadnienia bezpieczeństwa informacji instytucji realizującej swoje procesy biznesowe z wykorzystaniem technologii teleinformatycznych wyraża się w podporządkowaniu wszelkich działań potrzebom procesów biznesowych, które to potrzeby na wstępie należy zidentyfikować. Takie podejście określane jest również mianem „probiznesowego".

Bezpieczeństwo informacji w instytucji, rozumiane jako procesy ochrony integralności, dostępności i poufności informacji, tworzy pewien system, czyli zbiór elementów i zachodzących między nimi relacji. Zarządzanie tym systemem w instytucji ma zapewnić jej bezpieczeństwo na ustalonym dla niej poziomie. Należy podkreślić, że informacja powinna być zawsze odpowiednio chroniona bez względu na to, czy występuje:

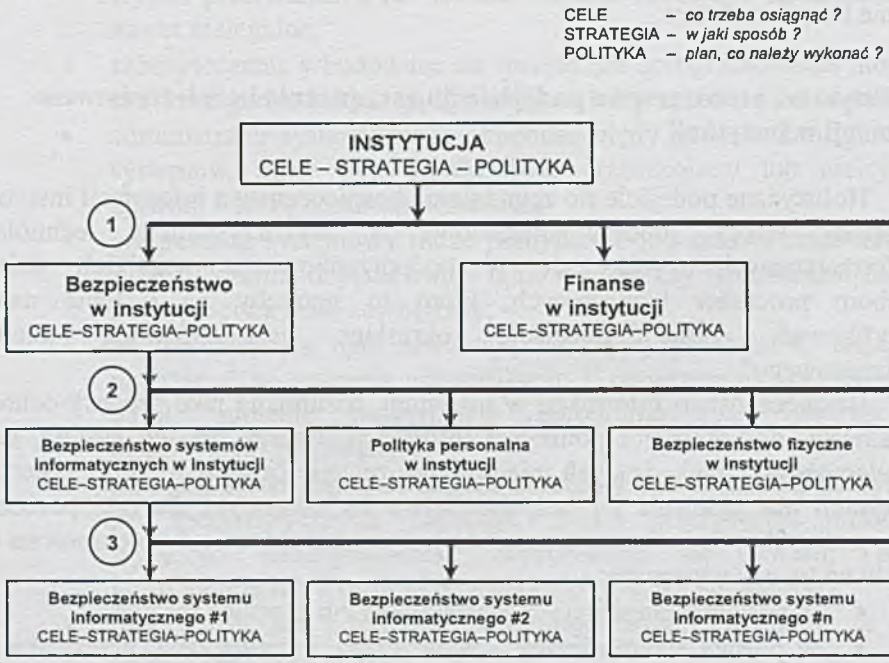
- w postaci papierowej – wydrukowana lub zapisana ręcznie,
- w postaci elektronicznej – wytwarzana, przetwarzana, przesyłana lub przechowywana elektronicznie,

- jako zapis audio lub video, czy jest przekazywana ustnie, np. podczas rozmowy bezpośredniej lub telefonicznej.

Podejście holistyczne, probiznesowe [8] jest często silnie akcentowane w standardach, zwłaszcza w najnowszych. Już w normie PN-ISO/IEC 13335-1 wprowadzono trójpoziomowy model hierarchii celów, strategii i rodzajów polityki (Rys. 1), w którym założono, że cele wyższego poziomu przekładają się na strategie niższego oraz pokazano, jak funkcjonowanie instytucji można rozpatrywać w kontekście jej bezpieczeństwa teleinformatycznego oraz bezpieczeństwa poszczególnych jej systemów.

Model ten wyraża holistyczne podejście do bezpieczeństwa instytucji, zarówno komercyjnych, jak i instytucji administracji publicznej czy służby zdrowia. Stanowi on wytyczną, jak konstruować system bezpieczeństwa od ogółu do szczegółu. Jest traktowany jako model referencyjny dla szczegółowych wytycznych zawartych w wielu standardach.

Podstawowymi i najczęściej obecnie stosowanymi standardami są ISO/IEC 27001 oraz ISO/IEC 27002 (dawniej ISO/IEC 17799), a także inne pomocnicze należące do tej rodziny. Pierwszy z wymienionych przedstawia szkielet systemu zarządzania bezpieczeństwem informacji, czyli SZBI (*ang. ISMS – Information Security Management System*) zgodny ze schematem zarządzania PDCA, czyli Plan-Do-Check-Act (Planuj – Wykonaj – Sprawdzaj – Działaj), opracowanym przez Deminga (Rys. 2) oraz zbiór zabezpieczeń. Drugi z nich dostarcza wskazówek (wzorcowych praktyk), jak stosować te zabezpieczenia.



Rys. 1. Model trójpoziomowy – hierarchia celów, strategii i rodzajów polityki [8]

Pozostałe normy tej rodziny, obecnie w różnym stadium opracowania, to:

- ISO/IEC 27000 Information security management system fundamental and vocabulary – wprowadzenie i terminologia,
- ISO/IEC 27003 Information security management system implementation guidance – przewodnik implementacji systemu zarządzania bezpieczeństwem informacji z rozszerzonymi informacjami na temat użycia wspomnianego modelu PDCA,
- ISO/IEC 27004 Information security management measurements – metryki i instrukcje dotyczące techniki pomiaru efektywności działającego systemu ISMS,
- ISO/IEC 27005 Information security risk management – zarządzanie ryzykiem bezpieczeństwa informacji; zasoby i ich wartościowanie; podatności związane z zasobami; zagrożenia wykorzystujące potencjalne podatności; metody oceny i postępowania z ryzykiem,
- ISO/IEC 27006 Requirements for bodies providing audit and certification of ISMS – wytyczne do prowadzenia audytu.

System ISMS (SZBI) jest rozumiany jako część całościowego systemu zarządzania instytucji, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji w instytucji. Dla ISMS podstawą jest więc podejście procesowe i zarządzanie ryzykiem.

Rys. 2. Schemat ogólny PDCA systemu zarządzania bezpieczeństwem informacji

Każda z faz PDCA (Rys. 2) systemu typu ISMS posiada swój własny zbiór procesów zarządzania. W załączniku A do ISO/IEC 27001 zaproponowano ponad 1000 różnego rodzaju zabezpieczeń, pogrupowanych wokół celów zabezpieczeń i umieszczonych w 10 rozdziałach załącznika (od A.5 do A.15):

A.5 Polityka bezpieczeństwa
- A.5.1 Polityka bezpieczeństwa informacji

A.6 Organizacja bezpieczeństwa informacji
- A.6.1 Organizacja wewnętrzna
- A.6.2 Strony zewnętrzne

A.7 Zarządzanie zasobami
- A.7.1 Odpowiedzialność za zasoby
- A.7.2 Klasyfikacja informacji

A.8 Bezpieczeństwo zasobów ludzkich
- A.8.1 Przed zatrudnieniem
- A.8.2 Podczas zatrudnienia
- A.8.3 Zakończenie lub zmiana zatrudnienia

A.9 Bezpieczeństwo fizyczne i środowiskowe
- A.9.1 Obszary bezpieczne
- A.9.2 Bezpieczeństwo sprzętu

A.10 Zarządzanie systemami i sieciami
- A.10.1 Procedury eksploatacyjne i zakresy odpowiedzialności
- A.10.2 Zarządzanie usługami dostarczanymi przez strony trzecie
- A.10.3 Planowanie i odbiór systemu
- A.10.4 Ochrona przed szkodliwym oprogramowaniem
- A.10.5 Kopie zapasowe
- A.10.6 Zarządzanie bezpieczeństwem sieci
- A.10.7 Obsługa nośników
- A.10.8 Wymiana informacji
- A.10.9 Usługi handlu elektronicznego
- A.10.10 Monitorowanie

A.11 Kontrola dostępu
- A.11.1 Wymagania biznesowe wobec kontroli dostępu
- A.11.2 Zarządzanie dostępem użytkowników
- A.11.3 Odpowiedzialność użytkowników
- A.11.4 Kontrola dostępu do sieci
- A.11.5 Kontrola dostępu do systemów operacyjnych
- A.11.6 Kontrola dostępu do aplikacji i informacji
- A.11.7 Przetwarzanie mobilne i praca na odległość

A.12 Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych
- A.12.1 Wymaganie bezpieczeństwa systemów
- A.12.2 Poprawne przetwarzanie w aplikacjach
- A.12.3 Zabezpieczenia kryptograficzne
- A.12.4 Bezpieczeństwo plików systemowych
- A.12.5 Bezpieczeństwo w procesach rozwoju i obsługi informatycznej
- A.12.6 Zarządzanie podatnościami technicznymi

A.13 Zarządzanie incydentami związanymi z bezpieczeństwa informacji
A.13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwa informacji
A.13.2 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami
A.14 Zarządzanie ciągłością działania
A.14.1 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
A.15 Zgodność
A.15.1 Zgodność z przepisami prawnymi
A.15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna
A.15.3 Rozważania dotyczące audytu systemów informacyjnych.

Przeglądając powyższy zbiór zabezpieczeń można z całą pewnością stwierdzić, że reprezentują one różnorodne aspekty: teleinformatyczne (A.10-A.12), fizyczno-środowiskowe (A.9) oraz organizacyjne (pozostałe), a przez to wyrażają holistyczne podejście do samego problemu bezpieczeństwa informacji.

Zarządzanie bezpieczeństwem informacji opiera się na zarządzaniu ryzykiem. Również i w tym przypadku podejście do ryzyka musi być holistyczne – uwzględniać wszelkie możliwe jego aspekty [8]. Rozpatrywane są zasoby, zagrożenia, podatności o różnym charakterze oraz szacowane są następstwa szkodliwych dla instytucji zdarzeń. Ponadto zagadnienia bezpieczeństwa informacji należy rozważać wraz z zarządzaniem ciągłością działania i usługami IT [9].

3. Holistyczne podejście do konstruowania i oceny zabezpieczeń teleinformatycznych

Wiadomo, że systemy teleinformatyczne i ich komponenty, wykorzystywane do realizacji procesów biznesowych instytucji podlegają różnym zagrożeniom w środowisku eksploatacji, stąd ich konstruktorzy wbudowują w nie różnego typu zabezpieczenia. I tu pojawia się problem, na ile można ufać tym zabezpieczeniom, że w należyty sposób ochronią zasoby informacyjne i usługi IT instytucji związane z realizacją jej procesów biznesowych? Od czego zależy skuteczność tych zabezpieczeń? Jak dobrać produkt lub system teleinformatyczny do własnych zastosowań o wystarczającej zdolności do obrony przed atakiem? Te i podobne pytania są rozstrzygane na gruncie dyscypliny projektowania i oceny zabezpieczeń o określonym poziomie tak zwanego uzasadnionego zaufania (*ang. assurance*). Tematyka ta jest związana ze standardem ISO/IEC 15408 Common Criteria (CC), czyli ze standardem „Wspólne kryteria do oceny zabezpieczeń teleinformatycznych". Również i w tym przypadku można zaryzykować stwierdzenie o holistycznym podejściu do bezpieczeństwa informacji reprezentowanym przez ten standard.

Standard Common Criteria dotyczy konstruowania produktów teleinformatycznych (sprzętu, oprogramowania, w tym układowego) oraz

zbudowanych z nich systemów teleinformatycznych, zwanych ogólnie przedmiotami oceny (*ang. TOE – Target of Evaluation*), które posiadają jakiekolwiek zabezpieczenia swych funkcji użytkowych, czyli zaimplementowane tak zwane zaufane funkcje zabezpieczające (*ang. TSF – Trusted Security Functions*), a które to zabezpieczenia powinny cechować się uzasadnionym zaufaniem. Pojęcie to oznacza przekonanie, że produkt lub system IT, zwany TOE, spełnia wyspecyfikowane dla niego cele zabezpieczeń. Zaufanie nie jest bezpodstawne, lecz zależy od tego, w jakich warunkach produkt powstawał, jak szczegółowo był specyfikowany, analizowany, testowany, dokumentowany, itd., czyli zależy od rygoryzmu dotyczącego projektowania, wytwarzania i eksploatacji TOE. Im większy rygoryzm, tym zaufanie do produktu lub systemu IT jest większe, jednak koszt takich TOE również rośnie.

Uzasadnione zaufanie jest mierzalne w zakresie od EAL1 do EAL7, gdzie EAL oznacza poziom uzasadnionego zaufania (*ang. Evaluation Assurance Level*). Uzasadnione zaufanie deklarowane dla produktu lub systemu IT poddawane jest wnikliwej ocenie przez niezależnych ekspertów w akredytowanym laboratorium. Po pozytywnej weryfikacji procesu i wyników oceny przez organizację nadzorującą laboratorium wydawany jest certyfikat poświadczający, że TOE spełnia warunki dla deklarowanego przez konstruktorów EAL.

Przedmiotami oceny mogą być:

- środki sprzętowe, np. kryptoprocesory,
- oprogramowanie (w tym układowe), np. szyfrator plików,
- ich kombinacja, np. system operacyjny współpracujący z kartami inteligentnymi,
- programy użytkowe, aplikacje, np. bazodanowe,
- narzędzia do rozwoju produktów,
- całe systemy.

Należy zauważyć, że nie zawsze są to typowe produkty bezpieczeństwa, lecz produkty posiadające funkcje zabezpieczające. Zakres produktów jest ogromny, dotyczy wszelkich wytworów informatyków i elektroników – od prostych edytorów tekstu po systemy dystrybucji kluczy kryptograficznych dla komputerów kwantowych.

Holistyczne podejście do tworzenia certyfikowanych produktów dotyczy wielu aspektów związanych z TOE i jego dokumentacją. Dotyczy fazy konstruowania, oceny w laboratorium i eksploatacji w środowisku pracy. Podczas konstruowania przedmiotu oceny rozpatrywane są jego własności bezpieczeństwa z uwzględnieniem zakładanego środowiska eksploatacji. Założenia dla tego środowiska są traktowane podczas oceny jako dogmaty, które w każdym rzeczywistym środowisku pracy muszą być spełnione. Rozpatrywane są wszelkie możliwe zagrożenia dla TOE i jego środowiska oraz zasady polityki bezpieczeństwa, które powinny być spełnione przez użytkowników TOE w tym środowisku [10-13].

4. Ochrona informacyjnej infrastruktury krytycznej

Współczesne, rozwinięte społeczeństwa korzystają na co dzień z rozbudowanych i skomplikowanych infrastruktur technicznych, wytworzonych przez te społeczeństwa. Przykłady takich infrastruktur to: produkcja i dystrybucja energii oraz różnego typu paliw, infrastruktura telekomunikacyjna, obsługa finansowa, zaopatrzenie w wodę i żywność, infrastruktura ochrony zdrowia, czy też zarządzanie państwem. Infrastruktury takie noszą miano infrastruktur krytycznych (*ang. CI – Critical Infrastructure*). Ich krytyczność polega na tym, że degradacja, uszkodzenie lub zniszczenie takiej infrastruktury ma krytyczne następstwa dla funkcjonowania państwa, jego gospodarki, a także zdrowia, pozycji ekonomicznej lub bezpieczeństwa jego obywateli [14]. Tak więc z uwagi na ogromne znaczenie infrastruktur krytycznych dla normalnego funkcjonowania państwa, społeczeństwa i jego rozwoju cywilizacyjnego, konieczna jest specjalna ochrona tych infrastruktur.

Na ochronę infrastruktury krytycznej *(ang. CIP – Critical Infrastructure Protection*) składa się szereg programów i działań podejmowanych przez właścicieli infrastruktur, ich producentów, użytkowników i operatorów, jednostki naukowo-badawcze, administrację rządową oraz jednostki odpowiedzialne za właściwe ich działanie. Celem tych przedsięwzięć jest utrzymanie funkcjonowania krytycznych infrastruktur w przypadku wystąpienia awarii, ataków lub incydentów, jak też zminimalizowanie skutków tych zdarzeń lub czasu niezbędnego do przywrócenia właściwego działania infrastruktur [14].

Funkcjonowanie infrastruktur krytycznych opiera się na zaawansowanych technologiach teleinformatycznych. Niektóre infrastruktury krytyczne, np. związane z usługami telekomunikacyjnymi, są zbudowane wyłącznie w oparciu o technologie teleinformatyczne. Zarówno infrastruktura o charakterze teleinformatycznym (np. dostawca usług internetowych), jak i infrastruktura innego typu (np. energetyka, dystrybucja paliw płynnych, rozliczenia między bankami) mogą posiadać procesy o charakterze krytycznym, takie jak procesy wytwarzania, przetwarzania, przesyłania i przechowywania informacji. Dlatego wprowadzono pojęcie krytycznej infrastruktury informacyjnej (*ang. CII – Critical Information Infrastructure*). Pod nazwą tą kryją się procesy informacyjne, wspomagane przez technologie informatyczne i telekomunikacyjne, będące same w sobie infrastrukturami krytycznymi lub niezbędne do funkcjonowania innych infrastruktur krytycznych [14].

Równolegle do pojęcia ochrony infrastruktury krytycznej (*CIP – Critical Infrastructure Protection*) istnieje nieco węższe pojęcie ochrony krytycznej infrastruktury informacyjnej (*ang. CIIP – Critical Information Infrastructure Protection*), gdzie zakres działań podanych w definicji CIP ograniczony zostaje do zagadnień teleinformatycznych.

Zagadnienie ochrony infrastruktury krytycznej musi być rozpatrywane holistycznie w wielu aspektach [15-18]. Rozpatrując aspekt zagrożeń, uwzględniane są:

- zagrożenia o charakterze zewnętrznym, rozważane na gruncie bezpieczeństwa teleinformatycznego (*ang. IT security*),
- zagrożenia o charakterze wewnętrznym, rozpatrywane z punktu widzenia teorii i praktyki wiarygodności systemów (*ang. dependability*), w tym bezpieczeństwa funkcjonalnego (*ang. safety*); istotną rolę odgrywają tu techniki: tolerowania uszkodzeń (*ang. fault tolerance*), zapewniające przetrwanie infrastruktury w sytuacji zagrożenia (*ang. survivability*) lub jej samodzielne przywrócenie do pełnej sprawności (*ang. self-healing*) [16].

Innym przejawem podejścia holistycznego jest interdyscyplinarność i globalny zasięg problematyki. Infrastruktury krytyczne wychodzą poza granice państw, tak więc istnieją zależności pomiędzy infrastrukturami poszczególnych państw. Dodatkowo, jedna infrastruktura może mieć wielu właścicieli, zarówno przedstawicieli sektora państwowego, jak i prywatnego. Dlatego nie można zapewnić niezakłóconego funkcjonowania infrastruktury wyłącznie w oparciu o jednego właściciela lub jeden kraj – konieczna jest współpraca międzynarodowa. Kwestia ta nabiera ważności w świetle nasilających się ataków terrorystycznych. Dlatego ochrona krytycznej infrastruktury informacyjnej traktowana jest ze szczególną uwagą i podkreślany jest jej interdyscyplinarny i globalny charakter.

Tworzone i badane są różne, wielowarstwowe modele infrastruktur. W modelach symulacyjnych rozpatrywane są warstwy:

- warstwa fizyczna (*ang. physical layer*); obejmuje ona elementy techniczne infrastruktury, takie jak np. urządzenia do produkcji i dystrybucji energii, paliw, gazu, zaś dla infrastruktur o charakterze teleinformatycznym obejmuje systemy wykorzystywane do realizacji usług informatycznych lub telekomunikacyjnych;
- warstwa logiczna (*ang. cyber layer*); zawiera ona systemy automatyki, systemy do kontroli i nadzoru typu SCADA (*ang. supervisory control and data acquisition*) oraz specjalistyczne systemy sieciowe;
- warstwa operatora; (*ang. organization layer*); w jej skład wchodzą systemy teleinformatyczne do wspomagania zarządzania infrastrukturą w zakresie wydajności jej funkcjonowania, efektywności ekonomicznej oraz reagowania na zdarzenia kryzysowe;
- warstwa strategiczno-biznesowa (*ang. strategic business layer*); obejmuje ona systemy teleinformatyczne różnego typu instytucji krajowych i międzynarodowych, zaangażowanych w koordynację współpracy infrastruktur i wypracowujących dla nich politykę działania (*ang. policy makers*).

W oparciu o modele symulacyjne prowadzone są analizy dwóch podstawowych typów zależności występujących w infrastrukturach:

- zależności poziomych (*ang. inter-dependencies*) między obiektami danej warstwy należącymi do różnych infrastruktur; przykładem takiej analizy jest badanie wpływu awarii sieci energetycznej na funkcjonowanie bankowego centrum przetwarzania danych;

- zależności pionowych (*ang. intra-dependencies*) między obiektami różnych warstw danej infrastruktury; przykładem analizy tego typu zależności może być badanie wpływu uszkodzenia systemu kontroli poziomu jakości usług telekomunikacyjnych na realizację procesów biznesowych przez dostawcę usług internetowych.

Prace naukowo-badawcze nad ochroną infrastruktur krytycznych prowadzone są w trzech kierunkach. Podejście analityczne (*ang. analytical approach*) sprowadza się do badania zachowania struktur (przewidywanie scenariuszy zdarzeń, określenie odporności struktur i liczbowych parametrów niezawodnościowych). Podejście rozpatrujące infrastrukturę jako system systemów (*ang. complex system / cybernetic approach*) skupia się na zrozumieniu istoty zachowania systemów złożonych. Wreszcie podejście symulacyjne (*ang. simulation approach*) dotyczy badania charakteru zależności poziomych i pionowych w strukturach.

5. Wnioski i uwagi końcowe

Ze względu na złożony charakter zagadnienia bezpieczeństwa, problemy z nim związane wymagają wielokierunkowych działań o różnym charakterze. Można je więc określić jako „holistyczne". System zarządzania bezpieczeństwem informacji, zależnie od potrzeb, wielkości i charakteru instytucji, wymaga ponadto skorelowania z innymi współistniejącymi w niej systemami zarządzania:

- procesami biznesowymi,
- usługami IT (ISO/IEC 20000),
- ciągłością działania (BS 25999),
- bezpieczeństwem funkcjonalnym (ISO/IEC 61508),
- jakością (ISO 9001),
- środowiskiem (ISO 14000),
- a nawet, bezpieczeństwem i higieną pracy (ISO 18000).

Procesy biznesowe instytucji realizowane z wykorzystaniem technologii teleinformatycznych mogą zostać przerwane lub zakłócone przez wiele czynników o niezwykle zróżnicowanym charakterze. Wynika stad, że do walki z tymi zagrożeniami stosowane muszą być również zróżnicowane środki określane mianem zabezpieczeń. Najczęściej w celu ochrony przed konkretnym zagrożeniem aplikowany jest zbiór różnorodnych zabezpieczeń. Często też jest stosowana ochrona wielowarstwowa. System bezpieczeństwa należy koniecznie ukierunkować na potrzeby procesów biznesowych i oprzeć się na wynikach analizy ryzyka. Każde z tych działań wyraża holistyczny charakter zagadnienia bezpieczeństwa informacji.

Literatura

1. Łukawiecki R.: Holistyczny pogląd na temat bezpieczeństwa przedsiębiorstwa, Strategic Consultant, Project Botticelli Ltd., 2005.

2. Ramsey Hamilton C.: The Case for Holistic Security: The Integration of Information and Physical Security as an Element of Homeland Security, RiskWatch.
3. Blount S.: Security Management: A New Model to Align Security With Business Needs, CA Security Solutions, 2006.
4. Bakman A.: A Strategic Approach to Gramm-Leach-Bliley Act Compliance - Ensuring Compliance and Security on the IT Infrastructure, Ecora Software.
5. Our Holistic Security Model, Reseller Club, 2007, www.resellerclub.com
6. McLaughlin L.: Holistic Security – interview with Tom Leighton, cofounder and chief scientist of Akamai Technologies and a professor of applied mathematics at MIT, IEEE Security & Privacy, vol. 3, no. 3, 2005, pp. 6-8.
7. Kopaliński W.: Słownik wyrazów obcych i zwrotów obcojęzycznych, Wiedza Powszechna, Warszawa 1968.
8. Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwa Naukowo-Techniczne, Warszawa 2006, 2007.
9. Białas A.: Development of an Integrated, Risk-based Platform for Information and E-services Security, In: Górski J.: Computer Safety, Reliability, and Security, 25th International Conference SAFECOMP2006, Springer Lecture Notes in Computer Science (LNCS4166), Springer Verlag Berlin Heidelberg New York 2006, ISBN 3-540-45762-3, pp. 316-329.
10. Bialas A.: Semiformal framework for ICT security development, The 8th International Common Criteria Conference, Rome, 25-27 September 2007 (publikacja w materiałach konferencyjnych w wersji elektronicznej).
11. Białas A.: A semiformal approach to the security problem of the target of evaluation (TOE) modeling, In: Arabnia, H. R., Aissi S. (Editors), Vert G. L., Williams P.A.H. (Associate Co Editors), Proceedings of the 2006 International Conference on Security and Management (The World Congress In Applied Computing - SAM'06: June, Las Vegas, USA), ISBN# 1-60132-001-9, 2006, Publisher: CSREA Press, pp. 19-25.
12. Białas A.: Semiformal Approach to the IT Security Development In: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T.: Proceedings of the International Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2007, IEEE Computer Society, Los Alamitos, Washington, Tokyo, ISBN 0-7695-2850-3, pp. 3-11.
13. Białas A.: Modeling the Security Objectives According to the Common Criteria Methodology, In: Aissi S., Arabnia H. R. (Editors), Daimi K., Gligoroski D., Markowsky G., Solo A.M.G. (Associate Co Editors), Proceedings of the 2007 International Conference on Security and Management (The World Congress In Applied Computing - SAM'07: June, Las Vegas, USA), ISBN# 1-60132-048-5, 2007, Publisher: CSREA Press, pp. 223-229.
14. European CI^{2}RCO 6FP project, http://www.ci2rco.org
15. Bologna S., Beer T.: An Integrated Approach to Survivability Analysis of Large Complex Critical Infrastructures. W: Willi S., Haemmerli B., Pohl H.,

Posch R.: Proceedings of the Critical Infrastructure Protection (CIP) Workshop. Frankfurt a. M. 2003.
16. Schmitz W.: Modelling and Simulation for Analysis of Critical Infrastructures. W: Willi S., Haemmerli B., Pohl H., Posch R.: Proceedings of the Critical Infrastructure Protection (CIP) Workshop. Frankfurt a. M. 2003.
17. Białas A.: Using ISMS concept for critical information infrastructure protection. In: Balducelli A., Bologna S. (eds), Proceedings of the International Workshop on "Complex Network and Infrastructure Protection – CNIP'06", ENEA – Italian National Agency for New Technologies, Energy and the Environment, Rome, March 28-29, 2006, pp. 415-426.
18. Białas A.: Wprowadzenie do problematyki ochrony krytycznej infrastruktury informacyjnej – projekt CI2RCO, W: Niemiec A., Nowak J.S., Grabara J.K. (red.): Bezpieczeństwo systemów informatycznych, Polskie Towarzystwo Informatyczne – Oddział Górnośląski, 2006, pp. 37-46.

ROZDZIAŁ XIV

BEZPIECZEŃSTWO HOLISTYCZNE – KRYPTOWIROLOGIA, KWANTOWA KRYPTOGRAFIA ORAZ BIOMETRIA KLASYCZNA I BEHAWIORALNA

Adrian KAPCZYŃSKI

1. Wprowadzenie

We współczesnym świecie informacja stanowi zasób, który chroniony jest przed dostępem osób niepowołanych za pomocą coraz bardziej złożonych rozwiązań informatycznych. Jednakże technologia to tylko jeden z elementów całego systemu; nie sposób rozważać zagadnienia bezpieczeństwa informacji w oderwaniu od aspektów organizacyjno-prawnych. Dostrzegalny jest dominujący nurt, który jednoznacznie wiąże się ze stosowaniem podejścia holistycznego (ang. *Holistic approach*).

W ramach XXIII Jesiennych Spotkań Polskiego Towarzystwa informatycznego zrealizowano sesję zatytułowaną: „Bezpieczeństwo holistyczne". W ramach tej sesji znakomici specjaliści przedstawili aktualny stan dziedziny w obszarach: informatyki śledczej, zapewnieniu ciągłości działania, jak i mechanizmów ochrony. Jako przewodniczący sesji, skłoniłem się do poszerzenia spektrum omawianych tematów o te, które na chwilę obecną można określić jako będące w trakcie intensywnego rozwoju. Mowa tutaj o kryptowirologii, kwantowej kryptografii oraz biometrii klasycznej i behawioralnej.

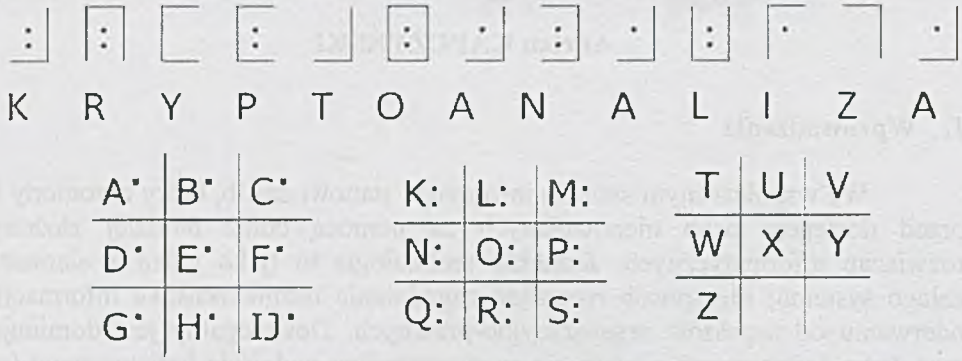
Zagadnienia te zostały w niniejszym rozdziale pokrótce przedstawione.

2. Kryptowirologia

Opracowany w roku 2001 w Chinach program złośliwy o nazwie „Nimda" był wyjątkowy, gdyż jego upowszechnienie realizowane było nie tylko za pośrednictwem plików wykonywalnych powielanych w ramach sieci komputerowej, ale również poprzez usługi internetowe oraz pocztę elektroniczną. Wraz z powstawaniem kolejnych, doskonalszych programów złośliwych, zaczęły powstawać coraz lepsze narzędzia ochrony – wśród nich oprogramowanie antywirusowe, które korzysta z rozwijanej na bieżąco bazy sygnatur oprogramowania złośliwego. Wykrycie programu złośliwego jest możliwe po przeprowadzonej analizie pod kątem zgodności z bazą sygnatur. Wschodzącym kierunkiem jest utrudnienie analizy programów złośliwych poprzez wykorzystanie mechanizmów kryptograficznych.

Do popularnych technik kryptograficznych zalicza się szyfry przestawieniowe i podstawieniowe (m.in. monoalfabetyczne, polialfabetyczne, homofoniczne, czy poligramowe). Jednym z przykładowych szyfrów

podstawieniowych jest szyfr cmentarny, korzystający z trzech macierzy w które wpisano litery alfabetu. Szyfrowanie wiąże się ze złokalizowaniem litery alfabetu w polu danej macierzy, a następnie przedstawienie jej w postaci symbolu graficznego, złożonego z identyfikatora macierzy oraz obramowania identyfikującego pole. Szyfrogram słowa „kryptoanaliza" stworzony za pomocą szyfru cmentarnego pokazano na rys. 1.



Rys. 1. Szyfr cmentarny jako przykład z zakresu klasycznej kryptografii

Mechanizmy kryptograficzne z biegiem lat ewoluowały i zostały dostrzeżone przez autorów programów złośliwych jako środek utajniania charakterystyk, umożliwiających identyfikację przez oprogramowanie antywirusowe. I tak zaczęto rozpatrywać dwa rozłączne obszary pod wspólnym terminem „kryptowirologia". Symbol kryptowirologii pokazano na rys. 2.

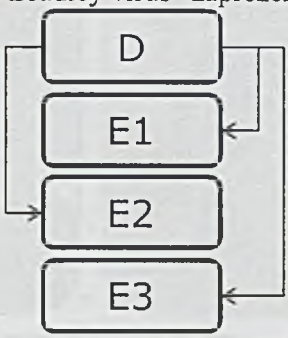
Rys. 2. Symbol rozwiązań kryptowirologicznych

Głównym celem kryptowirologii jest utrudnienie analizy programów złośliwych. Największym problemem kryptowirologów jest kwestia lokalizacji klucza kryptograficznego wykorzystywanego do odszyfrowania zawartości aktywnej programu złośliwego. W literaturze często przywoływany jest program złośliwy nowej generacji opracowany przez Filiola, o nazwie „The Bradley virus". Korzystał on dynamicznego klucza, zależnego od środowiska pracy programu. Architektura wzmiankowanego programu złośliwego obejmowała silnik odszyfrowujący (ozn. D – ang. deciphering engine) oraz bloki zaszyfrowane (E1, E2, E3). Każdy z bloków realizuje konkretne zadanie:

- E1 – uruchomienie modułu anty-antywirusowego,
- E2 – uruchomienie modułu infekcji,

- E3 – Inne (opcjonalne).

Składowe programu „The Bradley virus" zaprezentowano na rys. 3.



Rys. 3. Składowe rozwiązania kryptowirologicznego

Istotnym wyzwaniem stojącym przed kryptowiroanalitykami jest opracowanie mechanizmu ustalającego wartość klucza dynamicznego, jak również opracowanie metod analizy plików binarnych, umożliwiającej identyfikację programu złośliwego.

3. Kryptografia kwantowa

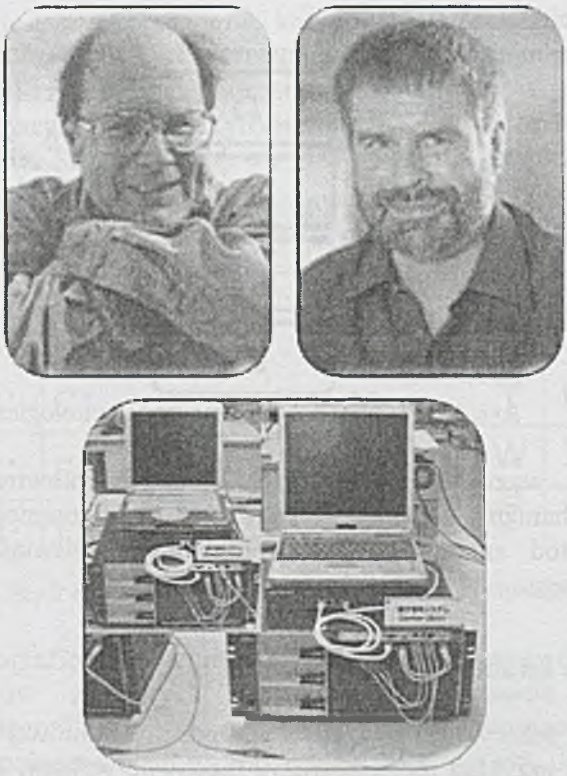
Potencjał leżący w obszarze kryptografii kwantowej jest coraz silniej eksponowany. Za przykład mogą posłużyć niedawne wybory, które zrealizowano w dniu 21 października 2007 roku w Szwajcarii. Otóż kluczowej zalety wynikającej z przekazu realizowanego za pomocą pojedynczych fotonów upatrywano w możliwości ustalenia czy dane zostały odczytane lub zmodyfikowane pomiędzy nadawcą a odbiorcą.

U podstaw współczesnych zastosowań leży opracowany przez Charlesa Bennetta oraz Gillesa Brassarda protokół BB84. Twórców protokołu BB84 oraz przykładowe stanowisko do kryptografii kwantowej przedstawiono na rys. 4.

Idea protokołu BB84 oparta jest na schemacie konsultacji klucza szyfrującego, a ten z kolei zakłada istnienie dwóch alfabetów: prostego (światło o polaryzacji 0° i 90°) oraz ukośnego (światło o polaryzacji 45° i 135°).

Konsultacja klucza między A oraz B przebiega według poniższego schematu:

- A wysyła do B fotony o losowo wybranej polaryzacji,
- B wybiera losowo bazy i przeprowadza pomiar polaryzacji otrzymanych fotonów,
- B informuje A jakie bazy zostały wykorzystane,
- A informuje B czy wybrane bazy były właściwe czy nie,
- A i B przechowują wyniki pomiarów zrealizowanych za pomocą właściwej bazy.



Rys. 4. Autorzy protokołu BB84 oraz stanowisko do kryptografii kwantowej

Zdolność do wytwarzania i detekcji stanów kwantowych stanowi podstawę rozwiązań z zakresu kryptografii kwantowej. Wspomniany protokół BB84 jest rozwijany, a jego praktyczne implementacje w warunkach realiów biznesowych w krótkim czasie będą pojawiały się coraz intensywniej.

4. Biometria klasyczna i behawioralna

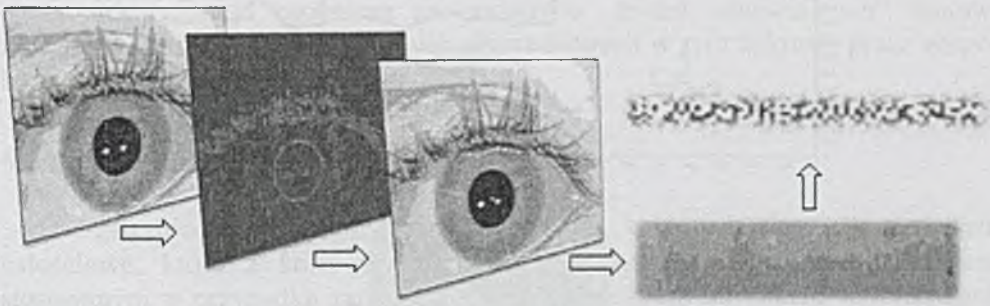
Metody biometryczne stanowią współcześnie stosowane środki kontroli logicznej i fizycznej. Wykorzystanie do identyfikacji lub weryfikacji tożsamości cech indywidualnych człowieka, takich jak wzór tęczówki oka, wzór linii papilarnych czy geometria dłoni (rys. 5) to obszar biometrii klasycznej. Metody biometryczne z roku na rok są coraz silniej eksponowane również w warunkach krajowych. Ośrodki akademickie (m.in. Politechnika Warszawska, Politechnika Wrocławska, Politechnika Śląska, Politechnika Szczecińska), badawczo-rozwojowe (m.in. Instytut Maszyn Matematycznych) oraz przedsiębiorstwa (m.in. Optel Sp. z o.o., AutoID Polska Sp. z o.o.) jednoznacznie prezentują zainteresowanie nie tylko badawczym, ale również aplikacyjnym charakterem biometrii klasycznej.

Rys. 5. Biometria klasyczna: tęczówki oka, linii papilarnych oraz twarzy

Wśród metod biometrii klasycznej do wyróżniających się należy zaliczyć biometrię tęczówki oka, której prekursorem jest John Daugman z University of Cambridge. Profesor Daugman przedstawił kolejne etapy procesu weryfikacji tożsamości na podstawie wzoru tęczówki oka:

- Wykonanie zdjęcia oka,
- Wyznaczenie obrazu kierunkowego,
- Ustalenie obszaru tęczówki oka,
- Akwizycja i transformacja uzyskanego obszaru,
- Uzyskanie binarnego kodu tęczówki oka (ang. *Iris code*),
- Porównanie uzyskane kodu z kodem referencyjnym.

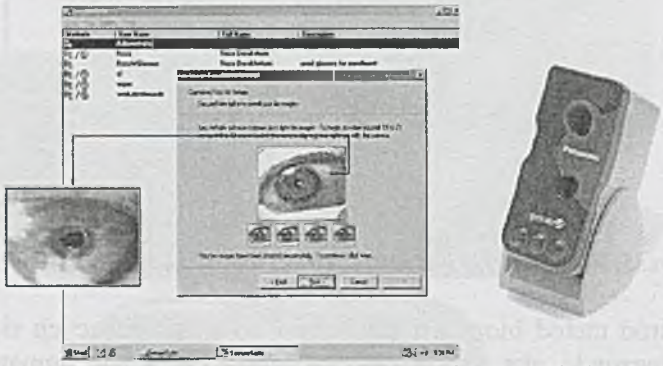
Wizualizacja procesu weryfikacji tożsamości została pokazana na rys. 6.



Rys. 6. Biometria tęczówki: od zdjęcia oka do kodu tęczówki oka

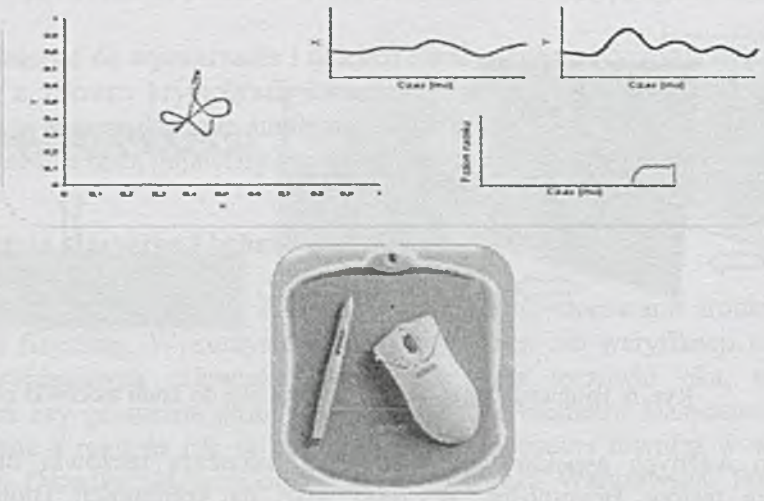
Do ważnych aspektów związanych z biometrią tęczówki oka należy zagadnienie testów żywotności. W 2003 roku na konferencji Biometrics w Londynie, prof. T. Matsumoto pokazał sposób na oszukanie stosowanych w praktyce gospodarczej systemów biometrycznych opartych o wzór tęczówki oka. Profesor Matsumoto wykorzystał nieskomplikowane podejście – wykonał zdjęcie oka, w którym w miejscu gdzie znajdujc się źrenica wyciął otwór. Następnie zdjęcie nałożył na oprawki okularów i z powodzeniem wykorzystał do weryfikacji tożsamości.

Eksperyment jak się okazało był powtarzalny i z powodzeniem udało się test przeprowadzić w warunkach laboratoryjnych dla kamery Panasonic BM ET 120 (patrz rys. 7).



Rys. 7. Problem testów żywotności tęczówki oka

Metody biometryczne bazują nie tylko na cechach anatomii, lecz również na cechach behawioralnych, m.in. dynamice pisania na klawiaturze, dynamice podpisu odręcznego czy też ruchu manipulatorem (np. z wykorzystaniem rękawicy sensorycznej). Dla skupienia uwagi przyjmijmy biometrię behawioralną podpisu odręcznego. W ramach tej biometrii analizowane są przebiegi w czasie składowych podpisu: współrzędna wertykalna, współrzędna horyzontalna, siła nacisku, kąt elewacji i kąt azymutu. Podpisy składane są na aktywnym tablecie graficznym (rys. 8.).

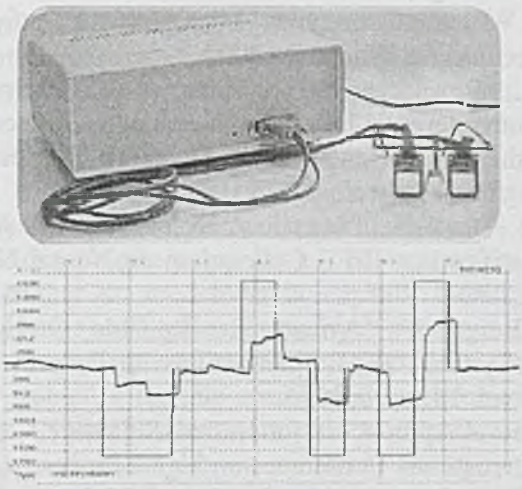


Rys. 8. Biometria behawioralna podpisu odręcznego

Do intensywnie rozwijanych biometrii behawioralnych należy biometria ruchu gałki ocznej. Pierwsze prace w Polsce zostały podjęte przez prof. J. Obera oraz jego współpracowników. Opracowany w ramach prac badawczych system OBER2 należy do rozwiązań sprzętowo-programowych, który był

wykorzystywany do identyfikacji osobniczej z oparciu o różne algorytmy klasyfikacji (m.in. drzewa C4.5 czy też sieci neuronowe). W ramach tej biometrii użytkownik śledzi punkt stymulacyjny przemieszczający się po ekranie monitora, a dzięki specjalnym okularom możliwa jest rejestracja danych dotyczących wychylenia oka lewego i prawego.

Sprzętowa warstwa systemu biometrii ruchu gałki ocznej wraz z zarejestrowanym przebiegiem w czasie wychylenia oka została pokazana na rys. 9.



Rys. 9. Biometria behawioralna ruchu gałki ocznej

Identyfikacja osobnicza na podstawie „źródeł odnawialnych" stanowi kluczowy kierunek prac badawczych prowadzonych w tym zakresie przez zespół biometrii Politechniki Śląskiej.

5. Podsumowanie

„Bezpieczeństwo holistyczne" to termin, który odzwierciedla podejście całościowe, które z kolei wydaje się być jedynym właściwym podejściem stosowanym w przypadku zarządzania bezpieczeństwem informacji w warunkach rzeczywistych (produkcyjnych).

W rozdziale przedstawiono trzy obszary związane z bezpieczeństwem holistycznym: kryptowirologię, kwantową kryptografię oraz biometrię. Zagadnienia te w wyraźny sposób wpisują się w nowe ujęcie tradycyjnych zagadnień bezpieczeństwem informacji, tj. kryptografii oraz uwierzytelniania.

Literatura

1. Barczak A., Sydoruk T.: Bezpieczeństwo systemów informatycznych zarządzania. Dom Wydawniczy Bellona, Warszawa 2003.
2. Bennett C.H., Brassard G. 1984: Quantum Cryptography: Public Key

Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers Systems and Signal Processing. Bangalore India.
3. Białas A.: Techniki szyfrowania. Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2001.
4. Białas A.: Podstawy bezpieczeństwa systemów teleinformatycznych. Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2002.
5. Białas A.: Podstawy szyfrowania. Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2001.
6. Denning D.: Wojna informacyjna i bezpieczeństwo informacji. Wydawnictwa Naukowo-Techniczne, Warszawa 2002.
7. Grzywak A.: Bezpieczeństwo systemów komputerowych. Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2000.
8. Han K., Sethi I. K.: Handwritting Signature Retrieval and Identification. Pattern Recognition Letters, vol. 17, 1996.
9. Hesketh G.B., Bhaler L., Porter J.: A Neural Network Approach to Automatic Signature Verification. IEEE Colloquium on Neural Networks for Industrial Applications, 1997.
10. Lee L.L., Berger T., Aviczer E.: Reliable On-line Human Signature Verification Systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, no. 6, 1996.
11. Lee L.L.: Neural Approaches for Human Signature Verification. Proceedings of the 3rd International Conference on Signal Processing, 1996.
12. Obaidat M.S., Sadoun B.: Verification of Computer User Using Keystroke Dy-namics. IEEE Transactions on Systems, Man and Cybernetics, vol. 27, no. 2, 1997.
13. Ober J., Kasprowski P.: Eye movement tracking for human identification. Proceedings of the 6th World Conference and Exhibition on Practical Application of Biometrics BIOMETRICS'2003. London, 2003.
14. Ober J., Kasprowski P.: With the flick of an eye. Biometrics Technology Today, vol. 12, March 2004.
15. Ober J., Kasprowski P.: Zastosowanie systemu pomiaru ruchu oka w biometrii. Techniki Komputerowe, Biuletyn Informacyjny, no. 1/2003. Instytut Maszyn Ma-tematycznych, Warszawa 2003.
16. Papamarkos N., Baltzakis H.: Off-line Signature Verification Using Multiple Neural Network Classification Structures. Proceedings of 13th International Conference on Digital Signal Processing, 1997.
17. Schneier B.: Kryptografia dla praktyków - protokoły, algorytmy i programy źródłowe w języku C. Wydawnictwa Naukowo-Techniczne, Warszawa 2002.
18. Stokłosa J. (red.): Ochrona danych i zabezpieczenia w systemach teleinformatycznych. Wydawnictwo Politechniki Poznańskiej, Poznań 2003.
19. Umpress D., Williams G.: Identity Verification Through Keyboard Characteris-tics. International Journal of Man-Machine Studies, vol. 23, Academic Press 1985.

ROZDZIAŁ XV

BEZPIECZEŃSTWO A UŻYWALNOŚĆ

Piotr KRAWCZYK

używalność
1. «przydatność do tego, żeby być używanym»
2. «możność korzystania z czegoś»
(Słownik języka polskiego PWN)

Używalność oznacza łatwość stosowania danej technologii . Oznacza ilość czasu lub pieniędzy, który użytkownik musi włożyć w jej zastosowanie. Inżynierowie niezbyt lubią pojęcie używalności, bo wprowadza do eleganckiego systemu niesforny i trudny do modelowania czynnik ludzki. Ludzie chętnie używają rozwiązań „używalnych", a unikają trudnych w użyciu.

Używalność skupia się na kwestii praktycznej – nie odpowiada na pytanie „czy da się to zrobić", tylko „ile czasu zajmie mi zrobienie tego" oraz „ile to będzie kosztowało". Często bowiem mamy do czynienia z sytuacją, w której pewną czynność **da się wykonać** (jest ona możliwa) ale jej nie wykonujemy, bo jest to nieopłacalne czasowo lub ekonomicznie.

Na przykład, można (da się) założyć stalowe drzwi klasy III do drewnianej komórki – ale jest to nieracjonalne jeśli koszt tego zabezpieczenia przekracza wartość samej komórki i jej zawartości. Przykład ten jest intuicyjnie zrozumiały bo dotyczy rzeczywistości, którą każdy może łatwo sam przeanalizować. W przypadku informatyki stopień skomplikowania technologii powoduje że nieraz sam projektant ma problem z określeniem granicy, po przekroczeniu której system przestaje być łatwy w użyciu[1].

Optymalna używalność wiąże się zawsze z pewnym kompromisem – na przykład między łatwością użycia a bezpieczeństwem. Podstawową wskazówką pozwalającą wyznaczyć miejsce tego kompromisu w przypadku rozwiązań związanych z bezpieczeństwem powinna być **analiza ryzyka**[2]. Jest to proces oceny potencjalnych zagrożeń dla danego systemu pozwalający podzielić je na „zagrożenia możliwe ale nieprawdopodobne" oraz „możliwe i prawdopodobne". Kosztowne zabezpieczenia stosujemy tylko dla tych ostatnich, zaś te „nieprawdopodobne" pozostają w sferze tzw. „ryzyka szczątkowego".

[1]Przykładem systemu pozornie łatwego do uruchomienia a w rzeczywistości najeżonego pułapkami opisało Internet Society Polska w swoim stanowisku na temat **wyborów powszechnych przez Internet** (http://www.isoc.org.nl/200701/wybory)

[2]**Analiza ryzyka** określa jakie możliwe ataki istnieją dla danego systemu, jaki jest koszt i potencjalny zysk włamywacza z każdego z nich. Jeśli koszt danego ataku jest znacznie wyższy od oczekiwanego zysku to z punktu widzenia atakującego będzie on nieopłacalny. Wdrażanie kosztownego zabezpieczenia przed tym atakiem jest więc nieuzasadnione.

Zabezpieczenie się przed wszystkimi zagrożeniami byłoby niezwykle kosztowne. W tym procesie nigdy nie należy jednak tracić z oczu horyzontu używalności.

Typowym przykładem z dziedziny technologii są **hasła**, którymi zabezpieczamy dostęp do systemu informatycznego. Hasło krótkie i łatwe do zapamiętania (np. „ala") jest łatwe w użyciu („wysoce używalne") – ale jest równocześnie łatwe do zgadnięcia. **Zbyt duża używalność oznacza w tym przypadku ryzyko narażenia użytkownika na szkodę.**

Naturalną odpowiedzią ze strony administratora systemu, któremu leży na sercu bezpieczeństwo użytkowników jest więc wymuszanie haseł długich i trudnych do zgadnięcia. W teorii bezpieczeństwo systemu będzie proporcjonalne do stopnia skomplikowania haseł. Czy rzeczywiście? Otóż nie – w praktyce, czego doświadczył każdy administrator systemu, po przekroczeniu pewnego poziomu skomplikowania użytkownicy nagle „wyłamią się" z tej zależności i zaczną „oszukiwać".

Na przykład będą przyklejać kartki z hasłami na obudowach monitorów, *de facto* sprowadzając ich bezpieczeństwo do zera. Jest to reakcja naturalna i całkowicie uzasadniona ze strony użytkowników, którym np. każe się zapamiętać hasła w rodzaju „Kr5o$x,8+Jt45".

Przykład ten jest szczególny, bo pokazuje jak użytkownik kreatywnie obchodzi wymyślone przez inżyniera ograniczenia całkowicie burząc misterną konstrukcję, której bezpieczeństwo na papierze mogło sprawiać wrażenie w pełni zagwarantowanego. Zamiast walczyć z brakiem używalności w ramach założeń systemu użytkownik po prostu „przeskakuje" na **inny poziom abstrakcji**, gdzie te założenia nie obowiązują. Czyli zamiast kombinować z mnemotechniką po prostu przykleja hasło na kartce do monitora.

Jest to przykład tego, jak **zignorowanie czynnika ludzkiego w całym systemie może zniweczyć doskonały technicznie plan i doprowadzić faktycznie do zniszczenia bezpieczeństwa systemu** zamiast jego podniesienia[3]. Tak dzieje się w sytuacji, gdy użytkownik ma możliwość takiego obejścia i nie grożą mu z tego tytułu specjalne konsekwencje.

Gdy użytkownik nie ma wyboru

Używalność jest kryterium, które można odnieść zarówno do technologii jak i prawa. Prawo jest jednak taką szczególną dziedziną życia, w której jego „użytkownik" czyli osoba podległa pod daną jurysdykcję nie ma specjalnego wyboru. Za uchylanie się od nakładanych przez prawo obowiązków grożą represje.

Co zatem robi użytkownik, który zostaje zmuszony do stosowania

[3]Oczywiście nie wolno nigdy zapominać o analizie ryzyka. W styczniu 2007 roku w jednym z polskich banków związek zawodowych oskarżył o mobbing administratorów, którzy zmuszali pracowników do stosowania trudnych do zgadnięcia haseł. W przypadku instytucji na której spoczywa taka odpowiedzialność jak bank brzmi to groteskowo – ale już wymuszanie bardzo trudnych haseł od użytkowników np. internetowego forum dyskusyjnego o luźnej tematyce byłoby nieuzasadnione.

nieużywalnego prawa? Jego wybór został radykalnie ograniczony, musi się więc dostosować. Ale jeśli przypomnimy sobie definicję używalności jako czasu i kosztu wymaganego do wykonania danej czynności to zrozumiemy, że to **dostosowanie odbywa się właśnie kosztem wykonywanej przez użytkownika pracy**. Zwiększy się więc udział czasu poświęcanego na obsługę obowiązków wynikających z przepisów zamiast na właściwą produkcję. Taki obowiązek musi być więc dobrze uzasadniony.

Regulacje prawne powinny pełnić **rolę służebną wobec człowieka** . Z patologią mamy do czynienia gdy zaczynają żyć swoim własnym życiem i rozrastać się do takiego stopnia, że zatracają właściwy cel dla jakiego zostały stworzone. Wraz z rozrostem rozmaitych regulacji instytucje, które je tworzą zaczynają się skupiać na tak niskopoziomowych detalach, że tracą obraz całości. W rezultacie z pozoru słuszne regulacje stają się przeciwskuteczne w szerszym kontekście.

Na przykład, jeśli **jeden** urząd nałoży na przedsiębiorców obowiązek comiesięcznego dostarczania różnych ankiet na temat pracy firmy to taki obowiązek wydaje się być niewielkim obciążeniem - wypełnienie ankiety zajmuje zaledwie 30 minut w skali miesiąca. Jest to niewiele i służy to konkretnemu celowi. Ale jeśli **sto** różnych urzędów zażąda od przedsiębiorcy takich ankiet? Z punktu widzenia **pojedynczego** urzędu wszystko jest w porządku – **ten urząd** zajmuje przedsiębiorcy tylko 30 minut i robi to w szczytnym celu. Ale z punktu widzenia przedsiębiorcy urzędy zabierają mu łącznie 3000 minut czyli 50 godzin w skali miesiąca. To bardzo dużo – to ponad tydzień roboczy.

W interesie państwa, które „zarabia" na podatkach czyli procencie od obrotu i zysku firmy leży, by wielkości tej „pańszczyzny" minimalizować z pożytkiem dla wszystkich.

Doskonałość a nadregulacja

Stwierdzenie, że wzrost gospodarczy jest korzystny, a nadregulacja mu nie sprzyja wydaje się oczywiste. Ale dotychczasowa praktyka w Polsce i w Unii Europejskiej zdaje się świadczyć, że **zrozumienie tego faktu zostało zatracone gdzieś po drodze do utopii, jaką jest prawo regulujące każdy aspekt rzeczywistości**.

Wydaje się, że u źródła tego zjawiska leżą jak najlepsze chęci, mające na celu realizację ideałów równości wobec prawa oraz jego precyzowanie. Rezultat takiego precyzowania jest w praktyce całkowicie odwrotny – do nadmiernie skomplikowanego prawa dostęp ma tylko wąska grupa osób, mogąca sobie pozwolić na zatrudnienie sztabu prawników i specjalistów. Zamiast równego dostępu do prawa mamy *deklarowany* równy dostęp i pogłębiającą się nierówność *faktyczną*.

Regulowanie różnych aspektów prowadzenia działalności gospodarczej jest koniecznością. Gdy okazuje się że obowiązujące regulacje nie wystarczająco opisują istniejącą rzeczywistość rynkową to mamy do czynienia z luką prawną.

Naturalnym procesem jest ich doprecyzowanie.

Ale wielokrotnie powtarzane doprecyzowanie w pewnym momencie prowadzi do opisywanego wcześniej stanu nadregulacji, w której przepisy stają się tak rozbudowane i szczegółowe, że wyłącznie dla ich obsługi powstaje oddzielna gałąź gospodarki[4].

Prawo nadmiernie rozbudowane to również prawo nieprecyzyjne i wewnętrznie sprzeczne. Przykładem może być polska ustawa o informatyzacji. Przy lekturze tej ustawy, rozporządzeń jej towarzyszących i ustaw przez nią znowelizowanych można odnieść wrażenie, że nikt tak na prawdę nie ogarnia całości stworzonych przez nie regulacji. Autorzy tworzący ją w ciągu kolejnych lat skupili się na zrozumieniu poszczególnych fragmentów, które nagle okazują się być wewnętrznie sprzecznymi jeśli spojrzy się na nie jako na elementy większej całości[5].

Studium nadregulacji – faktura elektroniczna

Przykładem regulacji, która miała dobre intencje ale okazała się chybioną jest wprowadzenie do polskiego prawa faktur elektronicznych. Ich stosowanie zostało dopuszczone rozporządzeniem ministra finansów w 2005 roku ale od tej pory ich wykorzystanie przez biznes jest minimalne. Dlaczego tak się stało?

Faktura elektroniczna miała być odpowiedzią na jeden z problemów fiskalizacji jakim są koszty fakturowania. Na koszt wystawienia jednej faktury składa się koszt jej wydrukowania, zapakowania, koszt samej koperty, koszt zawiezienia na pocztę, koszt przesyłki pocztowej itd. Można założyć że łącznie koszty te sumują się w granicach około 5 zł za fakturę. Są to koszty bezpośrednie – dodatkowym kosztem jest także czas konkretnego pracownika, który faktury musi wydrukować i wysłać. Zakładając, że firma miesięcznie fakturuje 1000 klientów koszt bezpośredni samego fakturowania wynosi minimum 5000 zł. Jest to koszt 1-2 etatów. Jest to przy tym koszt całkowicie jałowy – ani firma ani państwo nic na tych pieniądzach nie zyskuje.

Faktura elektroniczna miała ten koszt radykalnie obniżyć. Wysłanie faktury w formie elektronicznej przez Internet może kosztować bardzo niewiele, zwłaszcza że faktury i tak powstają w formie elektronicznej - większość firm używa do ich wystawiania odpowiedniego oprogramowania. Wysyłka może absorbować pracownika w stopniu nie większym niż wydanie systemowi dyspozycji „wystaw i wyślij faktury", a resztą zajmie się automat. W teorii wygląda to świetnie. Więc

---

[4]Przykładem może być np. działalność firm wyspecjalizowanych w pisaniu wniosków o dofinansowanie unijne – niezwykle rozbudowane wymagania wobec terminologii, języka, słów kluczowych i formy wniosków powodują, że mało który przedsiębiorca może to robić samodzielnie

[5]Ustawa o informatyzacji całym swoim duchem wydaje się regulować komunikację między podmiotami administracji publicznej. Tymczasem w art. 1 pojawia się ustęp 6 mówiący o regulowaniu komunikacji z podmiotami niebędącymi podmiotami publicznymi. W rezultacie nie za bardzo wiadomo kogo dotyczy ustawa.

dlaczego nie działa w praktyce?

Prześledźmy konstrukcję polskiego prawa dotyczącego faktury elektronicznej traktując jako podstawowe założenie jej cel – **obniżenie kosztów prowadzenia działalności gospodarczej**, co doprowadziłoby do zwiększenie konkurencyjności i zmniejszenie bezrobocia.

Możliwość stosowania faktur elektronicznych wprowadziło rozporządzenie ministra finansów w 2005 roku. Rozporządzenie to określa między innymi, że faktura musi być zabezpieczona **bezpiecznym podpisem elektronicznym** (wprowadzonym ustawą w 2001 roku). Jego celem jest ochrona autentyczności i integralności faktury – czyli na przykład uniknięcie sytuacji, w której odbiorca spodziewający się faktury otrzyma dokument sfałszowany, z podstawionym numerem konta. Cel ten jest w pełni uzasadniony.

Bezpieczny podpis w rozumieniu ustawy o podpisie elektronicznym wymaga bowiem posiadania **kwalifikowanego certyfikatu** (potwierdzonej oficjalnie elektronicznej tożsamości, i to jest uzasadnione) oraz – co istotne – **specjalnego oprogramowania i sprzętu** do jego składania. Oba wymogi są uzasadnione np. w przypadku elektronicznego podpisywania umów, bo podpis elektroniczny jest zgodnie z prawem równoważny podpisowi odręcznemu.

Jednak zastosowanie **tak silnego środka do tego konkretnego celu** spowodowało, że faktur elektronicznych przedsiębiorcy stosować **nie chcą bo jest to po prostu niepraktyczne**. Procedura składania *bezpiecznego* podpisu elektronicznego jest tak skomplikowana, że niweczy największą zaletą faktury elektronicznej czyli eliminację czynnika ludzkiego z procesu fakturowania. Jest to istotne, bo czynnik ludzki jest tutaj jednym ze największych kosztów.

W tym przypadku analiza ryzyka dla faktury elektronicznej nie wydaje się wskazywać na konieczność stosowania mechanizmu tak silnego prawnie jak bezpieczny podpis elektroniczny[6]. W praktyce nie zdarzają się przypadki zaprzeczenia wystawienia faktury przez wystawcę – taki „atak" nie ma tutaj sensu, a przed nim m.in. chroni właśnie bezpieczny podpis elektroniczny. Tymczasem w fakturze elektronicznej chodzi głównie o ochronę odbiorcy przed otrzymanie fałszywej faktury. Do zapewnienia tej ochrony wystarczający byłby zwykły podpis elektroniczny, nie wymagający specjalnego oprogramowania i sprzętu[7].

W rezultacie regulacja – choć cel miała szczytny – nie spełniła swojego zadania. Eskalacja wymagań wobec warunków jej stosowania spowodowała, że zatraciła swój podstawowy sens – używalność i opłacalność ekonomiczną.

---

[6]Dyrektywa unijna wprowadzająca faktury elektroniczne pozostawiła tutaj Państwom Członkowskim swobodę w wyborze między bezpiecznym a zwykłym podpisem elektronicznym, wychodząc z założenia że definicje jednego i drugiego mogą się znacząco różnić w różnych państwach.

[7]To że zastosowano podpis elektroniczny o wysokim poziomie bezpieczeństwa mogło być uzasadnione brakiem jakiejkolwiek "trochę słabszej" ale nadal bezpiecznej alternatywy. Planowana nowelizacja ustawy ma podobno taką formę wprowadzić.

Robimy tylko to co musimy

Przypadek faktury elektronicznej wskazuje też na inny problem związany z nadmierną regulacją. Przepisy o podpisie elektronicznym wprowadzają obowiązek, by wystawcy kwalifikowanych certyfikatów udostępniali użytkownikom darmowe oprogramowanie do ich weryfikacji. I znowu cel szczytny – a rezultat praktyczny bliski zeru.

Realizując literę rozporządzenia producent redukuje koszty tworząc oprogramowanie spełniające minimalne wymagania wynikające z wymogów prawnych – i ani jednej linijki kodu więcej. Rezultat jest taki, że udostępnione aplikacje (z jednym wyjątkiem), choć są w pełni zgodne z literą rozporządzenia są całkowicie nieużywalne. Jest to kolejna bariera dla stosowania podpisu elektronicznego.

Gdy państwo stwarza popyt

W latach 1999-2000 gdy Unia Europejska przygotowywała Dyrektywę 1999/93/EC, bezpieczny podpis elektroniczny miał być dla przedsiębiorców nie lada prezentem i miał przyczynić się do przegonienia gospodarki amerykańskiej, którą to myśl zawarto w pierwszej Strategii Lisbońskiej.

Dziś praktyczne wykorzystanie tych technologii w ramach dostarczonego przez Unię prawa jest szczątkowe. Problem ten nie dotyczy tylko Polski – właściwie we wszystkich Państwach Członkowskich bezpieczny podpis elektroniczny istnieje głównie na papierze. Jest to rezultat tego, że podpis elektroniczny potraktowano życzeniowo, jako objawowe leczenie problemów z konkurencyjnością unijnej gospodarki wynikającą m.in. z biurokracji i fiskalizacji, odpowiadających m.in. za wysokie koszty fakturowania.

Równocześnie starano się stworzyć rozwiązanie teoretycznie doskonałe i działające na wysokim poziomie abstrakcji. Takie rozwiązanie stworzono – ale nikt go nie używa. W prawnej i technicznej doskonałości tej konstrukcji zatracono bowiem jego sens – prostotę i niski koszt. Zapomniano, że to nie ono było celem samym w sobie – jest nim uproszczenie wymiany gospodarczej. Tego celu ta konstrukcja nie spełnia, stąd stagnacja podpisu w Unii[8]. **Jest on bardzo zaawansowany technicznie i prawnie, bardzo bezpieczny i bardzo... nieużywalny.**

W związku z tym w ciągu ostatnich lat pojawiły się inicjatywy legislacyjne służące **sztucznemu wykreowaniu popytu** na bezpieczny podpis elektroniczny w

[8]Przyczyn tej stagnacji jest wiele – m.in. taka, że na podstawie dość ogólnej dyrektywy każde Państwo Członkowskie stworzyło implementację odpowiednich przepisów według swojego pomysłu. W rezultacie w Unii istnieje kilkanaście wariantów techniczno-prawnych podpisu elektronicznego, wzajemnie niekompatybilnych co niweczy sens ich stosowania w handlu wewnątrzwspólnotowym. Podpis elektroniczny w Czechach to zupełnie co innego niż w Polsce, pomimo że wywodzą się z tej samej Dyrektywy. W związku z tym nie są kompatybilne prawnie ani technicznie.

celu, jak się wydaje, "przekonania" przedsiębiorców do korzystania z niego.

Pierwszym takim bodźcem miało być właśnie zastosowanie bezpiecznego podpisu do e-faktur. Jak widać przedsiębiorcy, którym **pozostawiono w tym przypadku wybór** (nie zmuszono ich do stosowania e-faktur) "zagłosowali nogami" i nie korzystają ani z podpisu ani z e-faktur. Jest to wybór w pełni racjonalny wobec nieużywalności tego podpisu w obecnej formie.

W ustawie o informatyzacji zawarto jednak drugi bodziec, tym razem nie pozostawiający wyboru. Przedsiębiorcy rozliczający się z ZUS będą **musieli** korzystać z podpisu kwalifikowanego od lipca 2008 roku, pomimo że dzisiaj funkcjonujący system oparty o darmowe certyfikaty nie sprawia problemów.

Wątpliwe jest jednak że w ten sposób przedsiębiorcy „przekonają się" do stosowania podpisu elektronicznego. Barierą w jego stosowaniu nie jest cena (ok. 500 zł). Barierą nie jest jakiś irracjonalny opór przed nowościami – rynek wymusza szybkie przyswajanie nowości technicznych.

Barierą jest po prostu nieużywalność podpisu elektronicznego w codziennych zastosowaniach.

Rozwiązania

Najważniejszym krokiem wydaje się uproszczenie i ograniczenie ilości produkowanego prawa. Choć wobec obowiązków legislacyjnych nakładanych przez Unię wydaje się to trudne, najważniejszym kryterium przy stanowieniu nowych przepisów powinna być ich zgodność z intencjami ustawodawcy – to znaczy, czy nowa regulacja zamiast uprościć, nie utrudni działalności gospodarczej.

Ustawodawcy nie wolno traktować przedsiębiorcy z założeniem, że nie wie on co jest dla niego dobre. A tak właśnie postąpiono z fakturami elektronicznymi i certyfikatami z ZUS. Jeśli przedsiębiorca nie stosuje przygotowanych "dla niego" udogodnień to ustawodawca powinien zastanowić się czy przypadkiem nie dlatego, że **nie nadają się** one do zastosowania.

Podstawowym krokiem do uzdrowienia polskiej gospodarki jest więc słuchanie głosu przedsiębiorców, którzy są głównym motorem polskiego wzrostu gospodarczego. Nowe regulacje prawne muszą być szeroko konsultowane w środowiskach tych podmiotów, których najbardziej dotyczą. Zwłaszcza te regulacje, które są tworzone z zamiarem "ułatwienia życia".

Konferencja Pracodawców Polskich w swojej „Zielonej Księdze"[9] pisze:

„Niezbędne byłoby wdrożenie systemu symulacji skutków zmian w prawie, oceny formułowanej ex ante, na etapie sporządzania listy inicjatyw legislacyjnych rządu."

Dalej KPP proponuje zwiększenie udziału konsultacji społecznych w

[9]Konfederacja Pracodawców Polskich (http://www.programppp.pl/doc/ZielonaKsiegaPanstwoPrzyjazne Pracodawcom.pdf), Konfederacja Pracodawców Prywatnych (http://www.pkpplewiatan.pl/upload/File/2007_03/czarna%20lista%20barier%202007.pdf)

procesie tworzenia prawa. Jest to bardzo istotna sugestia, która pozwoli uniknąć tworzenia prawodawstwa oderwanego od rzeczywistości i dławiącego rozwój gospodarczy.

Należy podkreślić, że choć w ciągu ostatnich dwóch lat bardzo wiele zmieniło się na lepsze w kwestii konsultowania ze środowiskiem prawa związanego z informatyzacją[10], to dużo jeszcze pozostaje do zrobienia.

Problemem na który zwraca uwagę KPP jest to, że komunikacja ta bywa często jednokierunkowa – to znaczy organizacje branżowe sugerują istotne zmiany, które są bez komentarza ignorowane.

Przy wprowadzaniu nowego prawa konieczne jest prowadzenie audytu prawnego w celu wykrycia ewidentnych problemów interpretacyjnych oraz sprzeczności z innymi aktami prawnymi.

Życzeniowy i odrealniony charakter kolejnych Strategii Lisbońskich wskazuje, że Komisja Europejska niekiedy produkuje zalecenia o charakterze utopijnym i ideologicznym. Problem polega na tym, że przekładają się one na konkretne obowiązki prawne i na konkretne koszty dla podatników.

Ustawodawca musi się więc powstrzymać się od bezkrytycznego i niekiedy nadgorliwego[11] wprowadzania regulacji na podstawie Dyrektyw unijnych, które pozostawiają sporą swobodę w interpretacji – można je wdrożyć w sposób mniej lub bardziej utrudniający życie.

Polska jako kraj o zadłużeniu przekraczającym 480 mln złotych nie może sobie pozwolić na eksperymenty społeczno-polityczne - potrzebuje więc prawa przejrzystego i przystającego do rzeczywistości.

[10]W dyskusji na temat prawa telekomunikacyjnego aktywny udział biorą obecnie stowarzyszenia PIIT, PTI, ISOC-PL i inne.

[11]Przykładami regulacji, które w Polsce zostały zaimplementowany w formie bardziej restrykcyjnej niż w unijnych Dyrektywach jest ustawa o podpisie elektronicznym, rozporządzenie o fakturach elektornicznych oraz projektowana nowelizacja prawa telekomunikacyjnego w zakresie retencji danych.

ROZDZIAŁ XVI

ODTWARZANIE SYSTEMU KOMPUTEROWEGO ORGANIZACJI PO WYSTĄPIENIU KATASTROFY

Andrzej M. MICHALSKI

1. Wprowadzenie

Podstawowe zadanie infrastruktury informatycznej, jakim jest zapewnienie dostępności informacji, wymaga w pierwszym rzędzie zapewnienie ciągłości działania wszystkich tych elementów, które tę dostępność zapewniają. Często wyróżnia się trzy poziomy ciągłości działania [WHENDI97]:

1. Wyeliminowanie pojedynczego punktu krytycznego (ang. Single Point of Failure), czyli wprowadzenie elementarnej redundancji.
2. Wykorzystanie serwerów wysokiej dostępności (ang. High Availability Servers).
3. Odporność na katastrofy (ang. Disaster Tolerance).

W dalszej części zostaną omówione zarówno czynniki, które mogą zakłócić ciągłość działania, jak i metody, pozwalające zapewnić nieprzerwaną pracę systemów.

Problemy, związane z bezpieczeństwem informacji i zapewnieniem wysokiego poziomu jej dostępności dotyczą przypadków, w których pojawia się sytuacja awaryjna, związana z niesprawnością systemu. Przyjęło się rozgraniczać dwa typy stanu braku lub ograniczenia dostępności do zasobów systemowych [MICHAL05]:

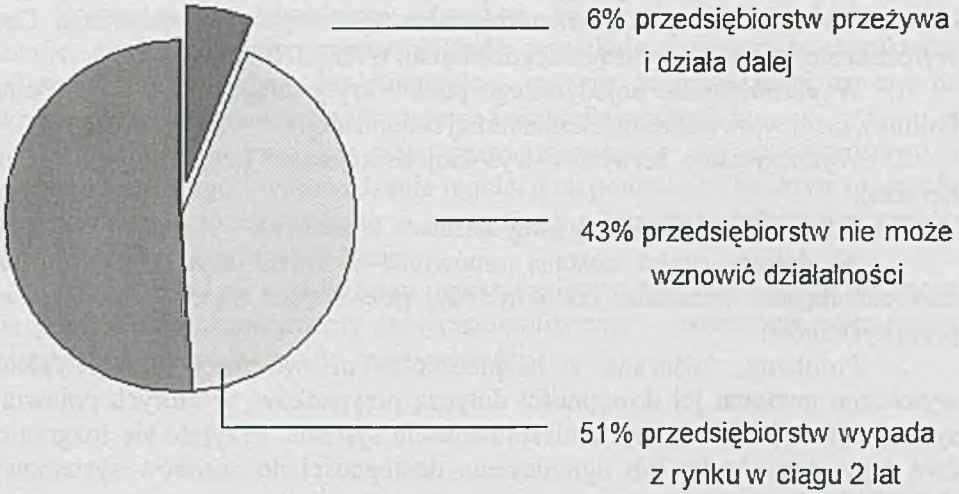
- awaria, kiedy uszkodzeniu ulega niewielki fragment systemu (w zakresie zasobów sprzętowych lub programowych, lub obu tych obszarów równocześnie), a do przywrócenia pełnej sprawności systemu wystarczają działania natury serwisowej,
- katastrofa, gdy uszkodzeniu lub całkowitemu zniszczeniu ulega większość istniejącej infrastruktury systemowej, a do przywrócenia sprawności systemu niezbędne są działania, związane z odtwarzaniem zniszczonych zasobów sprzętowych, nieruchomości, danych i często zasobów ludzkich.

We współczesnym świecie rosnącej liczby ataków terrorystycznych i pojawiających się na niespotykaną wcześniej skalę klęsk żywiołowych, wiele przedsiębiorstw uświadamia sobie realność wystąpienia katastrofy i musi dokonać ponownej analizy swojej polityki zabezpieczenia systemów komputerowych na wypadek jej zaistnienia i odtwarzania pracy systemu w celu przywrócenia ciągłości procesów biznesowych.. Jak mówi raport firmy konsultingowej Gartner, po 11 września 2001 "... osoby, odpowiedzialne za podejmowanie decyzji w przedsiębiorstwach, zaczynają w coraz większym stopniu rozumieć wagę ciągłości

działań biznesowych: to od nich zależy przetrwanie przedsiębiorstwa" [NORTON05].

2. Niebezpieczeństwo utraty zasobów informacyjnych

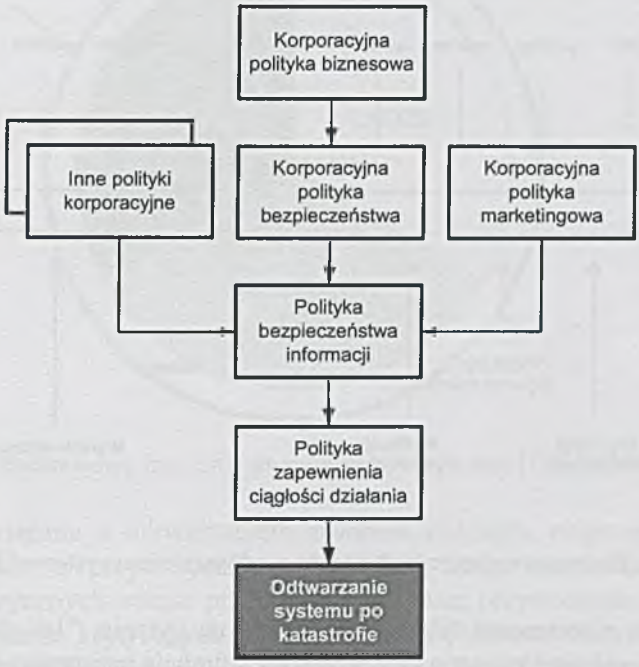
Przeprowadzone badania wskazują, że w przypadku utraty przez organizację swoich zasobów informacyjnych (np. w wyniku katastrofy), powrót przedsiębiorstwa do normalnych relacji rynkowych jest bardzo mało prawdopodobny - tylko ok. 6% takich przedsiębiorstw powraca do normalnego funkcjonowania, jak to przedstawia wykres na rys. 1 [WOŁOWS06].



Rys. 1. Sytuacja przedsiębiorstw, które utraciły swoje zasoby informacyjne [WOŁOWS06]

Jak zatem zapewnić ciągłość działań? Pierwszy z najistotniejszych czynników to wykorzystanie serwerów, opartych o nowoczesną architekturę, gwarantującą wysoki poziom dostępności mocy obliczeniowej. Drugim elementem są działania, związane z tworzeniem zapasowych kopii danych i przechowywaniem ich w geograficznie odległym miejscu, co w połączeniu z usługami backupu chroni przed utratą danych, gdy będzie miała miejsce katastrofa [NORTON05], [WEBSTE02]. Oba wymienione czynniki mają istotny wpływ na organizację i zarządzanie niemal każdej krytycznej aplikacji. Nieodzowne staje się staranne zaplanowanie działań, które winny być podjęte przed wystąpieniem katastrofy i po tym, gdy miała ona miejsce [CONTIN06], [CSOFUN06], [WOLDGH97]. Sedno przygotowań zawiera się w prawidłowo przeprowadzonych działaniach organizacyjnych [LIDERM06], [MICHAL06-2]. Odtwarzanie systemu po katastrofie stanowi jeden z elementów polityki bezpieczeństwa organizacji (rys. 2). Działania te wpisują się w politykę biznesową organizacji, których głównym celem

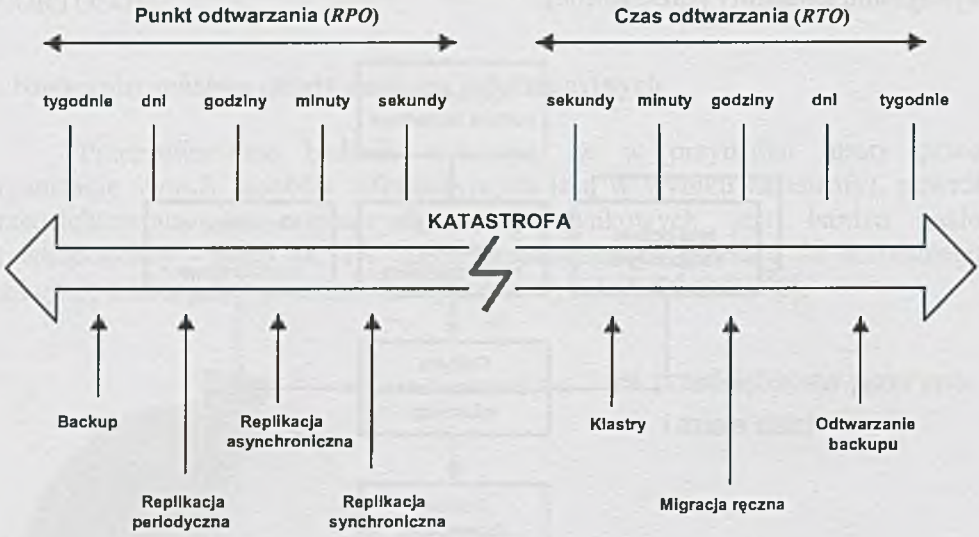
jest możliwe szybkie przywrócenie ciągłości procesów biznesowych po wystąpieniu katastrofy [LIDERM06].



Rys. 2. Hierarchia polityki działań organizacji [INFORM04]

3. Podstawowe pojęcia

Katastrofa może być zdefiniowana jako niezaplanowane wydarzenie, które w istotny sposób dotyka działań biznesowych przedsiębiorstwa i związane jest z ryzykiem bankructwa firmy w wyniku utraty rynku, narażenia na procesy sądowe lub utraty zysków. Skutki katastrofy rozciągają się znacznie poza utratę (nawet skopiowanych) danych – zwykle dotyczą zniszczeń budynku, instalacji i/lub zniszczeń systemu komputerowego. Ma to miejsce zarówno w przypadku naturalnego kataklizmu, jak i działań ludzkich, jak np. atak terrorystyczny, zainfekowanie wirusem komputerowym czy też zablokowanie systemu [SUCCES04]. Podstawowe pojęcia, związane z działaniami odtwarzania systemu po katastrofie, przedstawiono na rys. 3. Dwa najważniejsze z nich, z punktu widzenia zarządzania zasobami informacyjnymi to Czas Odtwarzania (ang. Recovery Time Objective - RTO) i Punkt Odtwarzania (ang. Recovery Point Objective – RPO) [JAKUBI04].

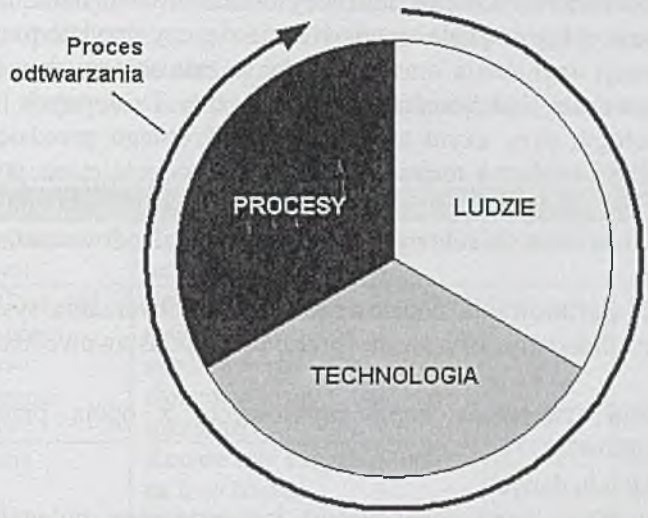


Rys. 3. Podstawowe pojęcia, związane z odtwarzaniem systemu [JAKUBI04]

Czas odtwarzania (***RTO***) odpowiada na pytanie: "Jak długo użytkownik może oczekiwać na ponownie dostępne dane i funkcje przetwarzania, zanim będzie miało to istotny wpływ na działanie przedsiębiorstwa?" Czas odtwarzania jest maksymalnym czasem po katastrofie, który jest niezbędny do przywrócenia działania wszystkich systemów, aplikacji i procesów biznesowych. Określając ten parametr należy doprowadzić do kompromisu między potencjalnymi stratami a kosztami rozwiązania, umożliwiającego najszybsze odtworzenie stanu sprzed awarii.

Natomiast ***Punkt Odtwarzania*** (***RPO***) określa następujący element: "Na jak dużą utratę danych może sobie pozwolić użytkownik?" Punkt odtwarzania to moment z przeszłości, w którym po raz ostatni została wykonana kopia danych i do którego momentu naszej działalności będziemy mogli wrócić (np. po awarii). Parametr ten dla różnych firm może mieć inną wartość - jednym wystarczy kopia sprzed tygodnia, inni zaś potrzebują danych sprzed kilkunastu sekund [FLORYS04].

Proces odtwarzania (często używany jest też termin przywracania) systemu po katastrofie obejmuje trzy podstawowe fazy [CZYMJE04] – odtworzenie czynnika ludzkiego, odtworzenie technologii i odtworzenie procesów (rys. 4).



Rys. 4. Podstawowe fazy procesu odtwarzania systemu [CZYMJE04]

Faza, związana z odtwarzaniem zasobów ludzkich, obejmuje działania, związane zarówno z przywróceniem niezbędnej kadry pracowniczej, jak i odtworzeniem fizycznych miejsc pracy. Następna faza, przywrócenia technologii, obejmuje odtworzenie krytycznych dla misji przedsiębiorstwa danych i aplikacji wraz ze sprzętem, niezbędnym do ich uruchomienia. Ostatnia faza związana jest z odtworzeniem wszystkich procesów biznesowych, niezbędnych do nieprzerwanego działania przedsiębiorstwa [HOWTOM03].

4. Technologie i procedury

Przy tworzeniu programu, zarządzającego działaniami niezbędnymi do zapewnienia ciągłości działania przedsiębiorstwa, należy wziąć pod uwagę wszystkie aspekty, które pozwolą kontynuować krytyczne procesy biznesowe w przypadku wystąpienia katastrofy. Obejmuje to zaplanowanie wytycznych organizacyjnych i wymagań logistycznych, opracowanie strategii projektowania, przygotowania, użytkowania i odtwarzania systemu komputerowego, a także uwzględnienie działań, związanych z konserwacją systemu oraz rozwojem i edukacją kadry. Program zapewnienia ciągłości działania systemu dotyczy załogi, nieruchomości i innych środków trwałych, procesów, zasobów wewnętrznych i zewnętrznych. Musi także uwzględnić markę i reputację firmy oraz jej przyszłość na rynku. Pojęcie ***odtwarzania systemu po katastrofie*** tradycyjnie związane jest z przywróceniem ciągłości usług informatycznych i w takim ujęciu stanowi podzbiór działań, zmierzających do zapewnienia ciągłości pracy przedsiębiorstwa.

Po zidentyfikowaniu czynników, niezbędnych do zapewnienia ciągłości działania organizacji, przychodzi pora na wybór, opracowanie i przetestowanie konkretnych rozwiązań, których zadaniem jest odtworzenie systemu

komputerowego i zapewnienie dostępności mocy obliczeniowej. Faza testowania jest niesłychanie istotna, gdyż pozwala na upewnienie się, czy przyjęte rozwiązania sprawdzą się w sytuacji zagrożenia oraz przebadanie zastosowanych technologii pod kątem ich efektywności funkcjonalnej i ekonomicznej. Dostępnych jest wiele różnorodnych technologii, przy czym zwykle dla konkretnego przedsiębiorstwa wybieranych jest kilka rozwiązań technologicznych jednocześnie, co pozwala w najlepszym stopniu osiągnąć uprzednio zdefiniowane cele w zakresie ochrony danych przedsiębiorstwa oraz docelowych wartości punktu odtwarzania i czasu odtwarzania systemu.

W przypadku definiowania docelowego punktu odtwarzania systemu, do dyspozycji mamy mechanizmy, oferowane przez dwie podstawowe technologie [SUCCES04]:

- backup (tworzenie kopii zapasowych, z opcją przenoszenia nośników);
- replikacja danych.

Backup (tworzenie kopii zapasowych) jest procesem, polegającym na tworzeniu dodatkowej kopii danych na taśmie magnetycznej lub na dysku. Skopiowana informacja stanowi obraz danych, odpowiadającej pewnej chwili z przeszłości, i w zależności od częstości realizacji tego procesu, nieaktualność danych może być liczona w godzinach, dniach lub tygodniach. Procesem tworzenia kopii zapasowych mogą być objęte wszystkie dane w całym przedsiębiorstwie i dbać należy o to, aby wszystkie dane były chronione z jednakową starannością, gdyż w przeciwnym wypadku łatwo może dojść do naruszenia obowiązujących przepisów lub utraty własności intelektualnej.

Backup z przenoszeniem kopii (ang. Vaulting lub PTAM) polega na tym, że uzyskane kopie zapasowe zostają zabrane z terytorium przedsiębiorstwa i są przechowywane w oddalonym, bezpiecznym miejscu, zwykle w ognioodpornych sejfach. Pojawiają się już wyspecjalizowane firmy, świadczące usługi w zakresie bezpiecznego przechowywania nośników danych. W rozwiązaniu tego typu konieczne jest opracowanie i wdrożenie precyzyjnego systemu identyfikacji poszczególnych taśm i ich lokalizacji oraz zarządzania procesami wymiany nośników przed wystąpieniem efektów zużycia się i starzenia.

Replikacja stanowi wyższy poziom zabezpieczenia danych i polega na kopiowaniu danych w czasie rzeczywistym na dodatkowe dyski, znajdujące się w odległej lokalizacji. Przy wyborze oprogramowania, pozwalającego realizować replikację danych, szczególną uwagę należy zwracać na jego niezależność od typu sprzętu i systemów operacyjnych. Zapewnia to określoną elastyczność przy aktualnych i przyszłych decyzjach sprzętowych oraz pozwala na wykorzystanie posiadanych zasobów w dłuższym horyzoncie czasowym. Zwykle mamy do czynienia z jednym z dwóch rodzajów replikacji (jest to uzależnione od trybu pracy):

- replikacja synchroniczna (dane zapisywane są równocześnie na oba nośniki – główny i zapasowy);

- replikacja asynchroniczna (dane na nośniku zapasowym zapisywane są z opóźnieniem, np. w chwilach mniejszej zajętości systemu wyrównywana jest zawartość obu dysków).

Podstawowe cechy przedstawionych technologii zawiera tabela 1.

Tabela 1. Technologie, pozwalające optymalizować punkt odtwarzania (RPO)

Technologia	Funkcjonalność	Media	Punkt odtwarzania
Backup (kopia zapasowa)	Kopiowanie danych na dysk lub taśmę	Dyski i/lub taśma	Dni
PTAM (Pick and Truck Access Method – przenoszenie nośników)	Przechowywanie taśmy ze skopiowanymi danymi w innej lokalizacji	Tylko taśma	Dni
Replikacja	Kopiowanie danych na inny obszar powierzchni dyskowej	Tylko dyski	Praktycznie na bieżąco (w ciągu milisekund)

Zródło: [SUCCES04]

W przypadku określania docelowego czasu odtwarzania systemu do wyboru mamy trzy podstawowe rozwiązania:

- technologia klastra;
- odtwarzanie z taśm magnetycznych;
- odtwarzanie z dysków.

Technologia klastra automatyzuje proces przywracania ciągłości zasobów pamięciowych, serwerów i aplikacji poprzez przekierowanie żądań dostępu od użytkowników (klientów) do innych zasobów, o ile zasoby podstawowe (pierwotne) uległy awarii lub zniszczeniu w wyniku katastrofy. Rozwiązania klastrowe gwarantują najwyższy poziom dostępności dla aplikacji krytycznych, poprzez dostarczanie mocy obliczeniowej z zasobów lokalnych lub zdalnych i mogą być zaimplementowane z wykorzystaniem różnych poziomów redundancji. Odpowiednio zaprojektowane rozwiązanie monitoruje stan zarówno zasobów sprzętowych, jak i aplikacji, i w przypadku awarii automatycznie podejmuje stosowne działania korygujące [MICHAL04-2].

Odtwarzanie z taśm magnetycznych jest procesem przywracania danych do stanu pełnej funkcjonalności, pochłaniającym zwykle najwięcej czasu i najbardziej podatnym na błędy.

Coraz częściej przedsiębiorstwa decydują się na ***odtwarzanie z dysków***, gdyż rozwój technologii sprzętowych doprowadził do tego, że ceny dużych macierzy dyskowych zaczęły być konkurencyjne w stosunku do systemów zabezpieczeń na taśmach. Jest to o tyle istotne, że technologia dyskowa znacznie skraca czas, niezbędny na odtworzenie informacji, co pozwala przywrócić funkcjonalność systemu już nie w ciągu dni, lecz godzin czy nawet minut.

Proces odtwarzania danych z taśm lub dysków po katastrofie może zostać radykalnie skrócony poprzez zastosowanie podejścia, zwanego odtwarzaniem "***na***

gołym komputer" (ang. "Bare metal restore"). Ten żargonowy termin oznacza udostępnienie (w przypadku katastrofy) nowego systemu komputerowego w innym miejscu, na którym następuje odtworzenie aplikacji i danych z nośników zapasowych. Duże firmy informatyczne w swojej ofercie posiadają już takie usługi, które polegają na utrzymywaniu w pełnej sprawności, dla potrzeb konkretnego klienta, systemu komputerowego, który w przypadku katastrofy jest udostępniany wraz z niezbędnymi pomieszczeniami, w celu jak najszybszego odtworzenia niezbędnych do zapewnienia ciągłości pracy przedsiębiorstwa usług informatycznych. Zwykle konfiguracja sprzętowa takiego systemu jest na bieżąco aktualizowana, aby w pełni była zgodna z konfiguracja systemu produkcyjnego, natomiast nie są instalowane produkty programowe – są one odtwarzane w procesie przywracania systemu z nośników zapasowych.

Omówione rozwiązania, stosowane do zapewnienia docelowego czasu odtwarzania, i ich cechy funkcjonalne zawiera tabela 2.

Tabela 2. Technologie, pozwalające optymalizować czas odtwarzania (RTO)

Technologia	Funkcjonalność	Media	Czas odtwarzania
Klaster	Praktycznie natychmiastowe odtworzenie systemu i aplikacji	Tylko dyski	Minuty
Replikacja	Automatyczne odtworzenie danych z niewielkim okresem postoju	Tylko dyski	Minuty, godziny
Odtwarzanie "na gołym systemie"	Automatyczne odtworzenie systemu i danych z pewnym okresem niedostępności	Dyski i/lub taśma	Godziny, dni

Źródło: [SUCCES04]

Podsumowanie

Pomimo tego, że administratorzy systemów informatycznych nie są w stanie zaplanować działań, przeciwdziałających wszelkim możliwym przerwom w pracy zarządzanych przez nich systemów, mogą – a nawet powinni – podejmować działania proaktywne, które pozwolą uniknąć całkowitej katastrofy infrastruktury informatycznej. Oczywiście, podstawą takich działań jest odpowiednie planowanie i przygotowanie zasobów oraz procedur [KHOSRO03]. Jednakże tylko wkomponowanie tych elementów (związanych z wystąpieniem katastrofy) w codzienne działania i procedury może zagwarantować, że przedsiębiorstwo przygotowane jest na najgorsze. Podstawowe kroki przygotowawcze powinny obejmować [NORTON05]:

- opracowanie spójnej strategii działań w przypadku wystąpienia katastrofy;
- wykrycie słabych punktów działania przedsiębiorstwa;

- analizę procesów pod kątem uniknięcia błędów w zarządzaniu;
- wdrożenie formalnej procedury komunikacyjnej na wypadek sytuacji kryzysowej;
- przetestowanie planu odtwarzania systemu po katastrofie;
- wybór odpowiednich dostawców sprzętu i oprogramowania.

Przechowywanie zapasowych nośników z danymi w innej lokalizacji nie uchroni przed wystąpieniem katastrofy, lecz pozwoli na ich odtworzenie, gdy dany oddział przedsiębiorstwa ulegnie zniszczeniu [KHOSRO03]. Natomiast wdrożenie procedury odtwarzania „na gołym systemie" pozwoli na uruchomienie wszystkich procesów biznesowych, nawet w przypadku całkowitego zniszczenia infrastruktury informatycznej przedsiębiorstwa.

Literatura

1. CONTIN06 - Continuity of Operations Planning and Business Continuity Planning, Mitretek Systems, http://www.mitretek.org/ContinuityOfOperationsPlanningAnd-BusinessContinuityPlanning.htm, August 2006.
2. CSOFUN06 - CSO Fundamentals: The ABCs of Business Continuity and Disaster Recovery Planning, CSOonline.com, http://www.csoonline.com/fundamentals/abc_continuity_pf.html, May 2006.
3. CZYMJE04 - Czym jest odtwarzanie po awarii i co można zrobić w tym zakresie?, e-Biuletyn Veritas, issue 1, Veritas Software Corporation, 2004.
4. FLORYS04 - Florys M.: Awarie struktury IT. Taniej zapobiegać, niż leczyć, Teleinfo nr 19, Warszawa 2004.
5. HOWTOM03 - How to maximize uptime within existing budget and manpower constraints, The Executive Perspective Series "The Economics of Availability", CMP Media LLC, Custom Media Solutions, USA, 2003.
6. INFORM04 - Information technology – Security techniques – Management of information and communications technology security, International Standard ISO/IEC 13335-1, 2004.
7. JAKUBI04 - Jakubik K.: Dane zawsze dostępne, NetWorld nr 3/4, Warszawa 2004.
8. KHOSRO03 - Khosrow-Pour M. (ed.): Advanced Topics in Information Resources Management, Vol. 3, Idea Group Publishing, USA 2003.
9. LIDERM06 - Liderman K.: Dokumentowanie systemu bezpieczeństwa teleinformatycznego - plan zapewniania ciągłości działania, artykuł opublikowany 3.2.2006 na portalu Centrum.Bezpeczeństwa.Pl, dostępny pod adresem http://centrum.bezpieczenstwa. pl/content/view/292/13, październik 2007.
10. MICHAL04 - Michalski A.: Server Solutions for High Performance Computing, in the monograph „Geographical Information Systems in Research & Practice", GIS Forum and University of Silesia, Zagreb 2004.

11. MICHAL05 - Michalski A.: System Disaster Recovery, rozdział w monografii "Geographic Information Systems in Research & Practice, IInd Part", GIS Forum i Uniwersytet Śląski, Zagrzeb, 2005.
12. MICHAL06 - Michalski A.: Odtwarzanie systemu komputerowego po katastrofie, Zeszyty Naukowe Politechniki Śląskiej 'Organizacja i Zarządzanie', z.38, Wydawnictwo Politechniki Śląskiej, Gliwice 2006.
13. NORTON05 - Norton D.: Administrator's Guide to Disaster Planning and Recovery, Third Edition, TechRepublic, USA 2005.
14. SUCCES04 - Successful Business Continuity Management and Planning with Veritas Consulting Services, Veritas White Paper „Solving the Business Problem of Downtime", Veritas Software Corporation, 2004.
15. WEBSTE02 - Webster J. and IBM Corp.: Step-by-step Data and Disaster Recovery, IBM Corp. and Illuminata Inc., 2002.
16. WHENDI97 - When disaster strikes... Will you be ready?, inform Special Insert, Issue 18, July/August 1997, Digital Equipment Corporation, Woburn MA, 1997.
17. WOLDGH97 - Wold G.H.: Disaster Recovery Planning Process, Disaster Recovery Journal, vol. 5, No 1 (Part I), No 2 (Part II) and No 3 (Part III), 1997.
18. WOŁOWS06 - Wołowski Fr.: Zarządzanie ryzykiem systemów informacyjnych, materiały XVIII Pełnoletniej Górskiej Szkoły PTI, Szczyrk 2006.

Nowoczesny handel to dzisiaj szybkość, oszczędność pieniędzy, ułatwienia logistyczne, płynny przepływ informacji, ale także wszystkie pułapki z tym związane. Aby ich uniknąć, umożliwiliśmy naszym klientom korzystanie z elektronicznej tożsamości.
Polska Wytwórnia Papierów Wartościowych S.A. od lat współtworzy w Polsce bezpieczne środowisko dla wymiany handlowej. Świadczy certyfikowane usługi oparte na technologii podpisu elektronicznego, umożliwia organizację bezpiecznych zakupów i przetargów elektronicznych, szkoli i doradza swoim Klientom.

Na rynku cyfrowych usług zajęliśmy pozycję **Zaufanej Trzeciej Strony** transakcji elektronicznych, współuczestniczącej w licytacjach i aukcjach oraz przetargach i zakupach jako gwarant absolutnego bezpieczeństwa w e-handlu.

Zarówno administracja publiczna, jak i kręgi biznesu zainteresowane są bezpiecznym wykorzystywaniem Internetu w działaniach handlowych. Właśnie z myślą o nich powołaliśmy Polską Platformę Przetargową (PPP). Korzystanie z niej pozwala na nowoczesną, kompleksową i oszczędną organizację procesu zaopatrzeniowego. Obejmuje ona elektroniczne zapytania ofertowe, licytacje, aukcje, zakupy z katalogów i raporty zakupowe. W odniesieniu do tradycyjnego nabywania towarów i usług, oszczędności przy zakupach drogą elektronicznych licytacji mogą sięgnąć nawet 50%. Zawdzięczamy to redukcji cen, a także usprawnieniu i skróceniu całego procesu zakupowego. Przetargi i zakupy dokonywane na platformie elektronicznej gwarantują całkowitą przejrzystość transakcji. Więcej informacji znajduje się na www.ppp.pwpw.pl.

Produkty i usługi Polskiej Wytwórni Papierów Wartościowych S.A. zawsze wyróżniały się najwyższą jakością i standardami bezpieczeństwa. Potwierdzają to przyznane firmie certyfikaty, m.in. ISO 9001, IQNet, ISO 14001.

W te standardy w pełni wpisuje się także utworzone w 2002 roku Sigillum Polskie Centrum Certyfikacji Elektronicznej. Sigillum PCCE jest jednym z trzech centrów certyfikacji w Polsce. Oferuje certyfikaty kwalifikowane, komercyjne, znacznik czasu oraz certyfikaty serwerowe. Sigillum PCCE aktywnie rozwija gamę oferowanych produktów, w których znajduje zastosowanie e-podpis. Do oferty należą m.in. systemy do elektronicznego fakturowania, elektroniczna skrzynka podawcza (Sigillum-ESP) oraz inne rozwiązania oparte o infrastrukturę klucza publicznego, projektowane pod indywidualne potrzeby klienta. Usługi Sigillum PCCE oferowane są podmiotom gospodarczym, instytucjom sektora publicznego oraz użytkownikom indywidualnym. Znajdują zastosowanie w transakcjach elektronicznych, zabezpieczeniu poczty elektronicznej i środowiska Internetu, wymianie dokumentów z urzędami, zawieraniu umów drogą elektroniczną, korespondencji z organami administracji publicznej czy zabezpieczaniu wewnętrznego obiegu dokumentów w przedsiębiorstwach i urzędach. Więcej informacji na www.sigillum.pl.

Nowe technologie znajdują coraz szersze zastosowanie. Zgodnie z obowiązującymi dziś wymogami każda placówka administracji publicznej jest zobligowana do udostępnienia elektronicznej drogi składnia podań i zapytań. System ESP – elektronicznych skrzynek

podawczych – pozwala na pełną kontrolę elektronicznych zgłoszeń od petentów. Gwarantuje także monitorowanie czasu udzielania odpowiedzi przez urzędy w ustawowych terminach.

W nowoczesnym przedsiębiorstwie obieg dokumentów papierowych generuje niepotrzebne koszty i zabiera czas. Projekt e- faktury umożliwia rezygnację ze stosowania tradycyjnych faktur i przejście na wymianę dokumentów elektronicznych. Nowe rozwiązanie pozwala na konfigurację oprogramowania „pod klucz", wg indywidualnych potrzeb klienta.

Ponad osiemdziesięcioletnie doświadczenie PWPW S.A. w produkcji banknotów oraz dokumentów zabezpieczonych było trwale związane z wypracowaniem odpowiedniej polityki bezpieczeństwa. Dlatego też biorąc pod uwagę tradycje i pozycję Polskiej Wytwórni Papierów Wartościowych S.A., spółki będącej w 100% własnością Skarbu Państwa, trudno w chwili obecnej znaleźć inny podmiot, który jako gwarant bezpieczeństwa w e-handlu umożliwia dostęp wszystkim zainteresowanym podmiotom do nowych, w pełni przejrzystych technologii.

Polska Wytwórnia

Papierów Wartościowych S.A.

Pl. Bankowy 2
00-095 Warszawa
tel. +48 (22) 531 27 52, fax. +4 (22) 531 27 53
e-mail: sigillum@pwpw.pl, aukcje@pwpw.pl
WWW.SIGILLUM.PL, WWW.PPP.PWPW.PL

Polska Wytwórnia Papierów Wartościowych S.A. ul. Romana Sanguszki 1, 00-222 Warszawa - wpisana jest do Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy, Sąd Gospodarczy XII Wydział gospodarczy pod numerem KRS 62594, NIP 525-000-10-90, wysokość kapitału zakładowego 130 650 380 zł, wysokość kapitału wpłaconego 130 650 380 zł.

Polskie Towarzystwo Informatyczne

Oddział Górnośląski

ul. J. Lompy 2/10, 40-040 Katowice
tel./fax: +48 32 2519811
www.pti.katowice.pl
Katowice@pti.org.pl

ISBN 978-83-60810-13-2