

Aleksandra CZUPRYNA-NOWAK
Politechnika Śląska, Wydział Organizacji i Zarządzania
Katedra Informatyki i Ekonometrii

DETERMINANTY SKUTECZNOŚCI ZINTEGROWANYCH SYSTEMÓW INFORMATYCZNYCH WYNIKAJĄCE Z SAMEGO SYSTEMU

Streszczenie. W artykule przedstawiono determinanty skuteczności zintegrowanych systemów informatycznych. Spośród nich wybrano najważniejsze dla grup badawczych.

DETERMINANTS OF EFFICIENCIES OF INTEGRATED COMPUTERIZED INFORMATION SYSTEMS FROM SYSTEM SUBSEQUENT

Summary. Determinant of efficiency of integrated computerized information system present in article. Most important choose among show determinant of efficiency of integrate computerized information system for research groups.

1. Wstęp

W chwili obecnej przedsiębiorstwa produkcyjne jak nigdy dotąd muszą poradzić sobie z problemem dostosowania się do otaczającej rzeczywistości. Stało się tak między innymi ze względu na zawirowania finansowe ostatnich kilku lat.

Reagowanie na zmiany nierozzerwanie wiąże się z podejmowaniem decyzji przez przedsiębiorstwa. Z kolei sprawne podejmowanie decyzji wymaga rzetelnej informacji o stanie przedsiębiorstwa. Gwarantem rzetelnej, dostarczanej decydom w odpowiednim czasie informacji dotyczącej przedsiębiorstwa jest sprawnie działający, zintegrowany system informatyczny.

Skuteczność działania zintegrowanego systemu informatycznego to możliwość odwzorowania wszystkich procesów zachodzących wewnątrz przedsiębiorstwa. Konsekwencją skutecznego działania jest jego sprawność, więc jeśli działanie jest skuteczne, to jest również sprawne. Sprawne działanie pociąga za sobą nie tylko skuteczność, ale również dokładność oraz ekonomiczność.

Celem artykułu jest przedstawienie najważniejszych determinant skuteczności zintegrowanego systemu informatycznego, odnoszących się do samego systemu.

Artykuł składa się z dwóch części. W pierwszej zostały przedstawione teoretyczne aspekty identyfikacji determinant skuteczności zintegrowanego systemu informatycznego. Druga część to wyłonienie najważniejszych spośród poddanych do badania determinant wśród grup badawczych.

2. Identyfikacja determinant

W obecnym czasie przedsiębiorstwa mogą dokonywać wyboru systemu spośród szerokiej gamy systemów zarówno polskich, jak i zagranicznych. Zakup znanych i cenionych na zachodzie systemów informatycznych może być znacznie utrudniony ze względu na koszt (IV/13). Producent systemu musi zadbać nie tylko o to, żeby system był dostosowany do polskiego prawodawstwa, ale przede wszystkim o to, żeby wszystkie funkcjonalne możliwości systemu uwzględniały cechy języka polskiego. W szczególności system powinien mieć [1]:

- dostępność polskiej wersji językowej łącznie z tekstem wszystkich interfejsów użytkowników, takich jak: ekrany do wprowadzania danych, podpowiedzi, zapytania i raporty,
- możliwość wprowadzania danych z polskimi znakami z klawiatury,
- dostępność pełnej dokumentacji systemu, jego modułów, procedur operacyjnych, opisu technicznego wraz ze słownikami danych, opisem procedur awaryjnych, opisem błędów i procedur ich usuwania,
- możliwość obsługi polskiej waluty oraz mechanizmy umożliwiające przeliczanie kursów walut, w przypadku gdy część transakcji przeprowadzanych w przedsiębiorstwie jest rozliczana w obcych walutach,
- zapewnienie terminowości wprowadzania unowocześnionej, polskiej wersji w przypadku unowocześnień dokonywanych w wersji oryginalnej.

Bardzo ważnym problemem wydaje się bezpieczeństwo systemu (IV/9), które jest miarą podatności na niepożądane zmiany i ingerencje [7]. Zadaniem systemów jest gromadzenie

i przetwarzanie informacji, których bardzo duża część to dane ściśle tajne, a od których bardzo często zależy przewaga konkurencyjna przedsiębiorstwa. W związku z tym powinny one być dostępne tylko i wyłącznie wybranej grupie użytkowników. Problem bezpieczeństwa danych jest bardzo skomplikowany i zależy od czynników: pozatechnicznych, organizacyjnych i administracyjnych. Najtrudniejsze do zidentyfikowania i zapanowania nad nimi są czynniki pozatechniczne, na które w dużej mierze nie ma się wpływu. Najczęstszym zabezpieczeniem, które stosują przedsiębiorstwa, jest personalizacja systemu (IV/10). Jest ono najczęstsze, ale jednocześnie najtrudniejsze do przestrzegania w przedsiębiorstwie. Dzieje się tak dlatego, że pracownicy nierzadko nie zdają sobie sprawy z zagrożeń, jakie niesie za sobą np. wymiana haseł dostępu czy udostępnianie swoich haseł innym osobom, w wyniku czego może dojść do utraty poufności danych, utraty dostępności czy integralności. Utrata poufności wiąże się z ujawnieniem informacji przetwarzanej przez system nieautoryzowanemu użytkownikowi. Utrata dostępności są to wszelkie zdarzenia mogące doprowadzić do braku dostępu w określonym czasie do systemu informatycznego, programu lub informacji dla autoryzowanych użytkowników. Utrata integralności natomiast są to zdarzenia mogące doprowadzić do nieautoryzowanej modyfikacji lub zniszczenia danych przetwarzanych przez system informatyczny.

Istnieją dwa standardy, które stanowią odniesienie dla oceny bezpieczeństwa systemu informatycznego. Pierwszy z nich to TCSEC, który został opublikowany przez Departament Obrony USA. W standardzie tym zostało zdefiniowanych siedem klas systemów: A1, B1, B2, C1, C2, C3, D. Najbezpieczniejszymi systemami są takie, które należą do klasy A, a najbardziej niebezpieczne to te, które należą do klasy D. W omawianym standardzie wymagania stawiane systemom zostały podzielone na następujące kategorie [7]:

- polityka bezpieczeństwa – zasady przydziału uprawnień do zasobów systemu,
- identyfikatory – zasady przydziału identyfikatorów do poszczególnych obiektów/ zasobów systemu,
- identyfikacja – zasady identyfikacji użytkowników systemu,
- rozliczenia – zasady identyfikacji użytkowników, śledzenia i monitorowania ich,
- pewność – rozwiązania i techniki projektowe, zmierzające do wiarygodnej i skutecznej realizacji deklarowanych rozwiązań,
- ciągła ochrona – rozwiązania zapewniające trwałość zaimplementowanych mechanizmów bezpieczeństwa.

Drugim obowiązującym standardem jest standard ITSEC, który powstał w Unii Europejskiej jako harmonizacja kryteriów wykorzystywanych w poszczególnych krajach europejskich. Standard ten obejmuje dwie klasyfikacje systemu. Pierwsza z nich jest związana z deklarowanymi właściwościami systemu, określającymi jego bezpieczeństwo, druga zaś związana jest z zapewnieniem, że poziom bezpieczeństwa zostanie osiągnięty.

Właściwości systemu mogą być konfrontowane z właściwościami zdefiniowanymi przez tzw. sponsora systemu, tzn. z właściwościami jednej z dziesięciu zdefiniowanych klas: F-C1, F-C2, F-B1, F-B3, IN, AV, DI, DC, DX. Według standardu definicja klasy bezpieczeństwa składa się z następujących sekcji:

- identyfikacja i uwierzytelnienie – zasady identyfikacji i metod uwierzytelnienia użytkowników,
- kontrola dostępu – wymagania dotyczące selektywnego dostępu do systemu,
- rozliczenia – wymagania dotyczące mechanizmów rejestracji informacji na potrzeby audytu,
- audyt – wymagania dotyczące mechanizmów rejestracji informacji na potrzeby audytu,
- ponowne użycie – wymagania dotyczące zapewnienia bezpieczeństwa w kontekście współdzielenia zasobów,
- dokładność – wymagania dotyczące mechanizmów zapewniających spójność i integralność danych,
- wiarygodność – wymagania dotyczące dostępności i niezawodności usług,
- wymiana danych – wymagania dotyczące mechanizmów transmisji danych.

Kolejnym, bardzo ważnym problemem jest otwartość systemów informatycznych na współpracę z innymi programami użytkowymi (IV/7). Otwartość systemu informatycznego oznacza, że istnieje możliwość rozszerzenia systemu o nowe moduły oraz łączenie go z systemami zewnętrznymi [2]. Niezbędne jest, aby systemy informatyczne umożliwiały współpracę np. z aplikacjami biurowymi (MS Office, OpenOffice).¹ Dostosowanie systemów informatycznych do pakietów biurowych niesie za sobą dodatkowe korzyści. Użytkownicy przyzwyczajeni do pracy z pakietami biurowymi szybciej nauczą się pracować ze zintegrowanym systemem informatycznym (IV/17). Dodatkowo, jeśli interfejs będzie przejrzysty (IV/18), szkolenia pracowników mogą znacznie się skrócić, co obniży koszty wdrożenia systemu.

Bardzo ważnym problemem zintegrowanych systemów informatycznych jest ich elastyczność (IV/1), i to zarówno funkcjonalna, jak i strukturalna. Elastyczność funkcjonalna przejawia się w maksymalnym dostosowaniu rozwiązań sprzętowo-programowych do potrzeb przedsiębiorstwa, elastyczność strukturalna natomiast to dynamiczne dopasowanie się do zmian zachodzących w trakcie eksploatacji systemu. Do niedawna systemy informatyczne były budowane na podstawie powiązanych ze sobą modułów (IV/15) ([2], [3]). Takie zorganizowanie systemu umożliwiało etapowe wdrażanie systemów. Jednak od pewnego

¹ Przykładem zintegrowanego systemu informatycznego dopasowanego do aplikacji biurowych jest system DUET, który powstał w wyniku współpracy firm Microsoft oraz SAP 5.

czasu pojawiły się systemy, w których budowa modułowa jest zastępowana skupieniem się na obsłudze procesów biznesowych. Rozwiązanie takie jest powiązane z koncepcją architektury SOA, która odzwierciedla nowe trendy w zarządzaniu.² W głównej mierze polega to na budowaniu architektury w pełni elastycznego oprogramowania z możliwością dostosowania go do zmieniających się warunków. Wdrożony system powinien zapewnić kompleksowość funkcjonalną, tzn. system swoim zakresem powinien obejmować wszystkie sfery działalności przedsiębiorstwa (IV/14).

3. Determinanty skuteczności systemów informatycznych – badania empiryczne

Determinanty skuteczności związane bezpośrednio z systemem informatycznym przedstawiono w tabeli 1. Badania nad skutecznością polegały na przeprowadzeniu ankiety w grupach: użytkowników i projektantów systemów informatycznych. W grupie użytkowników wyłoniono dwie podgrupy badawcze: kierowników oraz specjalistów, w grupie projektantów natomiast: analityków, projektantów, wdrożeniowców oraz programistów. Obie grupy poproszono o przyznanie punktów poszczególnym determinantom. Każdy z uczestników badania przyznawał pojedynczej determinancie od 0 do 10 punktów.

Obliczone średnie punkty w grupach badawczych pozwoliły wyłonić najważniejsze determinanty:

- w grupie kierowników – IV/5 – *rzetelność danych w systemie* (9,069),
- w grupie specjalistów – IV/9 – *bezpieczeństwo danych* (9,048),
- w grupie analityków – IV/5 – *rzetelność danych w systemie* (9,120),
- w grupie projektantów – IV/25 – *zgodność systemu z procedurami pracy obowiązującymi w danym przedsiębiorstwie* (8,821),
- w grupie programistów – IV/16 – *stabilność systemu informatycznego* (8,800),
- w grupie wdrożeniowców – IV/5 – *rzetelność danych w systemie* (9,400).

² SOA jest koncepcją tworzenia systemów informatycznych, w której główny nacisk jest kładziony na definiowanie usług spełniających wymagania użytkownika. Enterprise SOA jest nurtem reprezentowanym przez firmę SAP [5].

Tabela 1

Zestawienie obliczonych wskaźników zbieżności ekspertów

Oznaczenie	Nazwa determinanty
IV/1	Elastyczność systemu informatycznego
IV/2	Złożoność systemu informatycznego
IV/3	Czas dostępu do danych
IV/4	Cykl życia systemu
IV/5	Rzetelność danych w systemie
IV/6	Sposób powstania systemu
IV/7	Łączność systemu z otoczeniem
IV/8	Budowa hierarchiczna systemu
IV/9	Bezpieczeństwo danych
IV/10	Personalizacja systemu
IV/11	Rodzaj zastosowanej platformy sprzętowej
IV/12	Rodzaj architektury klient/serwer
IV/13	Koszt zakupu systemu
IV/14	Koszty obsługi systemu
IV/15	Integracja modułów systemu informatycznego
IV/16	Stabilność systemu informatycznego
IV/17	Łatwość obsługi interfejsu
IV/18	Przejrzystość interfejsu
IV/19	Prosta komunikacja z systemem
IV/20	Zgodność systemu z dyrektywami podatkowymi i kodeksem celnym UE
IV/21	Zgodność systemu z przepisami BHP
IV/22	Zgodność systemu z przepisami ZUS
IV/23	Zgodność systemu z normami ISO
IV/24	Zgodność systemu z normami ochrony środowiska
IV/25	Zgodność systemu z procedurami pracy obowiązującymi w danym przedsiębiorstwie
IV/26	Zgodność systemu z rzeczywistymi procesami zachodzącymi w przedsiębiorstwie
IV/27	Zgodność systemu z polskim prawodawstwem dotyczącym działalności gospodarczej
IV/28	Możliwość odwzorowania procesu produkcyjnego oraz procesów sterowania produkcją
IV/29	Możliwość dokonywania zmian systemu informatycznego
IV/30	Adaptacyjność systemów informatycznych
IV/31	Możliwość tworzenia nowych modeli w systemie
IV/32	Łatwość implementacji systemu w warunkach konkretnych wdrożeń

Źródło: Opracowanie własne

4. Wnioski

W artykule zaprezentowano wyniki badań nad skutecznością zintegrowanych systemów informatycznych w zarządzaniu przedsiębiorstwem produkcyjnym. Wyłoniono najważniejsze determinanty skuteczności systemów informatycznych według poszczególnych grup badawczych. Należy zwrócić uwagę na to, że przedstawiona w artykule – na podstawie

analizy literatury oraz badań empirycznych – lista czynników nie jest listą zamkniętą. Będzie ona ulegać zmianom wraz ze zmianami zachodzącymi w przedsiębiorstwie, zakresem wdrożenia systemu informatycznego czy też postawionym celem wdrożenia.

Temat artykułu ma charakter rozwojowy, gdyż pociąga za sobą wiele obszarów badawczych. Ciekawym kierunkiem badań wydaje się analiza poszczególnych determinant, mająca na celu ustalenie kierunku ich wpływu na skuteczność zintegrowanych systemów informatycznych. Dalsze badania powinny zmierzać również do prób normalizacji, która w konsekwencji doprowadzić może do próby konstrukcji wskaźnika skuteczności systemu informatycznego.

Bibliografia

1. Ćwikła G.: Zintegrowany system zarządzania dla firm o produkcji małoseryjnej – analiza wymagań, [w:] Knosala R.: Komputerowo zintegrowane zarządzanie. WNT, Warszawa 2004.
2. Kisielnicki J., Sroka H.: Systemy informacyjne biznesu. Informatyka dla zarządzania. Metody, projektowania i wdrażania systemów. Wydawnictwo Placet, Warszawa 2001.
3. Lenart A.: Zintegrowane systemy informatyczne klasy ERP. Teoria i praktyka na przykładzie systemu BAAN IV. Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2005.
4. Olszak C.M., Sroka H.: Zintegrowane systemy informatyczne w zarządzaniu. Wydawnictwo AE w Katowicach, Katowice 2001.
5. Sadecki B., Wolny W.: Tendencje rozwojowe systemów ERP – analizy na podstawie planów wybranych producentów oprogramowania, [w:] Knosala R.: Komputerowo zintegrowane zarządzanie. Tom II. WNT, Warszawa 2007.
6. Tałgarski J. (red): Przedsiębiorczość – rozwój firmy. Wydawnictwo AE w Krakowie, Kraków 1999.
7. Zalewski A., Cegiela R., Sacha K.: Modele i praktyka audytu informatycznego, <http://www.e-informatyka.pl/article/show/479> (27.11.2007).

Abstract

It present results of research in article over efficiency of integrated computerized information system in management productive enterprise. It show according to individual research groups most important determinants of efficiencies of computerized information systems.