PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 159
Informatyka Ekonomiczna 19 2011

Andrzej Bytniewski, Marianna Kowalska
Uniwersytet Ekonomiczny we Wrocławiu

CZYNNIK LUDZKI JAKO ŹRÓDŁO ZAGROŻEŃ W PROCESIE TWORZENIA I FUNKCJONOWANIA SYSTEMU INFORMATYCZNEGO W PRZEDSIĘBIORSTWIE

Streszczenie: Zasoby ludzkie stanowią jeden z ważniejszych elementów systemu informatycznego, dlatego też mogą być poważnym źródłem zagrożeń podczas procesu tworzenia i funkcjonowania tego systemu Zagrożenia te mogą powstawać na każdym etapie tworzenia systemu, mogą one pochodzić zarówno ze źródeł wewnętrznych przedsiębiorstwa, jak i jego otoczenia, to jest ze źródeł zewnętrznych. W artykule omawia się większość zagrożeń powstających już na etapie tworzenia systemu informacyjnego spowodowanych czynnikiem ludzkim.

Słowa kluczowe: czynnik ludzki, systemy informatyczne, zagrożenia systemów.

1. Wstęp

Szeroko rozumiana technologia informacyjna, w tym technologia informatyczna i teleinformatyczna, w znacznym stopniu na trwałe wpisała się we współczesne życie gospodarcze i społeczne.

Wykorzystanie systemu informatycznego w procesie zarządzania współczesnym przedsiębiorstwem wymaga zastosowania wysokiej jakości oprogramowania systemowego i użytkowego, a także odpowiednio wydajnego i niezawodnego sprzętu informatycznego.

Otoczenie rynkowe, w którym funkcjonują współczesne przedsiębiorstwa, charakteryzuje wysoka zmienność, nieprzewidywalność oraz rosnące wymagania, głównie co do poziomu zaspokajania potrzeb organizacji użytkującej system, ale też preferencji klientów przedsiębiorstwa (zwłaszcza nabywców dóbr i usług oferowanych przez przedsiębiorstwo). Globalizacja procesów gospodarczych oraz rosnąca konkurencja to tylko kilka czynników determinujących poszukiwanie przez przedsiębiorstwa coraz to nowszych, sprawniejszych systemów informatycznych zarządzania. Uzyskanie takich systemów możliwe jest dzięki przeprowadzeniu właściwego procesu ich tworzenia, na tym etapie bowiem powstaje wiele zagrożeń, a także później, w trakcie użytkowania.

2. Źródła zagrożeń w procesie tworzenia i funkcjonowania systemu informatycznego

W każdym przedsiębiorstwie, które korzysta z technologii informacyjnych, powstają różne rodzaje zagrożeń związanych z tworzeniem i funkcjonowaniem systemu informatycznego, a także z prowadzoną przez nie działalnością gospodarczą. Definiuje się je jako potencjalne, negatywne zdarzenia pojedyncze lub grupowe, przypadkowe lub celowe, które mogą spowodować lub powodują szkody w systemie informatycznym przedsiębiorstwa, a w konsekwencji i działalności przedsiębiorstwa. Zagrożenia te mogą wynikać z błędów i nadużyć ludzkich, błędów i awarii sprzętu oraz oprogramowania, a także zdarzeń losowych. Zagrożenia te wiążą się przede wszystkim z poszczególnymi elementami systemu informatycznego, takimi jak:
– zasoby ludzkie,
– zasoby informacyjne,
– zasoby proceduralne,
– zasoby techniczne.

Zasoby ludzkie stanowią potencjał wiedzy naukowo-technicznej i ekonomicznej ukierunkowanej na rozwiązywanie problemów systemu informacyjnego dla osiągnięcia celów, funkcji i zadań firmy [Nowicki 1999, s.15].

Do drugiej grupy należą zasoby informacyjne. Zasoby te zawierają zbiory danych przeznaczonych do przetwarzania oraz zbiory informacji przeznaczone dla odbiorców szczebli decyzyjnych. Zasoby informacyjne opisują więc fakty i zdarzenia związane z procesami gospodarczymi firmy. W zależności od klasy systemu informatycznego zasoby informacji mogą być zorganizowane w postaci baz danych, bazy metod, bazy modeli oraz bazy wiedzy.

Następna grupa to zasoby proceduralne. Tworzą one: algorytmy, procedury i oprogramowanie. Zasoby te umożliwiają wykorzystanie zasobów informacyjnych do realizacji między innymi zadań technologicznych czy programowych w ramach systemu informacyjnego [Kisielnicki, Sroka 1999, s. 35].

Kolejną grupę stanowią zasoby techniczne. Elementami tych zasobów są: sprzęt komputerowy, sieci telekomunikacyjne, nośniki danych. W ostatnich czasach zauważalna jest coraz bogatsza rynkowa oferta tych zasobów, zarówno pod względem rodzajowym, jakościowym, jak i cenowym. Specyfika prac wykonywanych przez sprzęt informatyczny determinuje w znacznym stopniu jego konfigurację i sposób wykorzystania.

Z zaprezentowanych elementów systemu informatycznego mogą wynikać różne zagrożenia. Zagrożenia te przejawiają się często utratą danych, które mogą wynikać z następujących przyczyn [*Utrata*…]:
– błędów człowieka,
– wirusów komputerowych,
– klęsk żywiołowych,

– problemów sprzętowych,
– błędów w oprogramowaniu.

Badania przyczyn utraty danych w systemach informatycznych prowadzi systematycznie firma Ontrack Data Recovery. Firma ta przeprowadziła globalną ankietę dotyczącą badania przyczyn utraty danych wiosną 2010 roku wśród 2000 respondentów z 17 krajów Europy, Azji, Ameryki Północnej, w tym również z Polski [*Utrata*…].

Dane z 2002 i 2010 roku, dotyczące przyczyn utraty danych w systemach informatycznych, przedstawiono w tabeli 1.

Tabela 1. Przyczyny utraty danych według opinii użytkowników systemów

Przyczyna utraty danych	Według opinii użytkowników (w %)			Szacunkowa ilość odzyskanych danych (w %)		
	2002[1]	2010	wskaźnik dynamiki 2010/2002	2002[2]	2010	wskaźnik dynamiki 2010/2002
Błąd człowieka	11%	40%	3,63	26%	27%	1,04
Wirusy komputerowe	2%	15%	7,50	4%	7%	1,75
Klęski żywiołowe	1%	3%	3,00	2%	3%	1,5
Problemy sprzętowe	78%	28%	0,35	56%	29%	0,52
Błędy w oprogramowaniu	7%	12%	1,72	9%	7%	0,78

Źródło: [*Understanding*...].

Według ankiety przeprowadzonej wśród użytkowników, spośród wszystkich przyczyn utraty danych największy odsetek stanowią przyczyny określone jako błąd człowieka. W roku 2010 wynosił on 40% i wzrósł aż 3,63 razy w stosunku do roku 2002 (wówczas wynosił 11%). Tak wysoki wzrost tego rodzaju błędu może być wynikiem zwiększonego skomplikowania użytkowanych systemów, braku doświadczonej kadry, niewłaściwej dokumentacji eksploatacyjnej systemu, nieprawidłowego parametryzowania systemów w czasie ich wdrażania itp.

Drugą najważniejszą przyczyną utraty danych były problemy sprzętowe, a udział ich wyniósł 28% w roku 2010 i 78% w roku 2002. W tym przypadku wskaźnik dynamiki wykazuje spadek tej przyczyny utraty danych aż o 65% i wynosi 0,35. Analizując wartość tego wskaźnika, należy przyjąć, że nastąpił istotny wzrost niezawodności sprzętu komputerowego, i można to uznać za pozytywny objaw postępu cywilizacji technicznej całej społeczności świata.

[1] Dane zacytowane z pracy [Woda] były pobrane z tej samej strony (www.ontrackdatarecovery.com/understanding-data-loss/), ale dotyczyły 2002 roku.

[2] Tamże.

Kolejną ważną przyczyną utraty danych są wirusy komputerowe, a ich udział wynosił 15% w 2010 roku, co stanowi 7,5-krotny wzrost w porównaniu z rokiem 2002 (tylko 2%). Podkreślić należy bardzo duży wzrost tego wskaźnika, będący skutkiem istotnego rozwoju sieci Internet i dużego przepływu zbiorów danych. Zastanowić się trzeba nad wprowadzeniem nowych regulacji prawnych w tym zakresie, aby w maksymalnym stopniu wyeliminować tę przyczynę.

Poważną przyczyną utraty danych są także błędy w oprogramowaniu; w 2010 roku ich odsetek wyniósł aż 12% . W porównaniu z 2002 rokiem (tylko 7%) nastąpił wzrost 1,72 razy. Analizując szerzej tę przyczynę, należy również zaliczyć ją do błędów człowieka. Błąd ten powstaje w procesie tworzenia systemu informatycznego. Spowodowane to jest, jak można przypuszczać, pospiesznym wprowadzaniem na rynek przez producentów niesprawdzonego, nieprzetestowanego oprogramowania. Wskazane jest w tym przypadku zwrócenie większej uwagi na procedurę tworzenia oprogramowania, jego testowania, parametryzowania, a następnie wdrażania. Niewłaściwa parametryzacja systemu w momencie jego wdrażania rodzi błędy, którym zazwyczaj nadaje się znamiona błędów w oprogramowaniu.

Ostatnią analizowaną przyczyną utraty danych są klęski żywiołowe. Przyczyna ta spowodowała w 2010 roku utratę 3% danych i w porównaniu z 2002 rokiem wzrosła 3-krotnie (w 2002 stanowiła tylko 1% utraty danych). Tak duży wzrost wynika z nasilenia się różnego rodzaju kataklizmów, które określane są ogólnie jako klęski żywiołowe. Przyczyna ta jest przypadkiem szczególnym ze względu na brak możliwości jej przewidzenia i zabezpieczenia się przed nią.

Biorąc pod uwagę poszczególne rodzaje przyczyn zagrożeń systemów informatycznych spowodowanych utratą danych, należy wskazać, że przyczyna spowodowana błędem ludzkim jest dominująca, bo wynosi aż 40%. Do niej w zasadzie należy jeszcze dodać, jak już wcześniej sygnalizowano, przyczynę określaną jako błędy w oprogramowaniu (12%). Obie przyczyny stanowią aż 52% utraty danych, co należy uznać za bardzo poważne źródło zagrożeń działania systemów informatycznych. Podkreślić należy, że utrata danych w systemach informatycznych wpływa w decydujący i negatywny sposób na sprawność działania przedsiębiorstwa i w związku z tym konieczne jest przywiązywanie ogromnej wagi do maksymalnej eliminacji przyczyn ją wywołujących.

Kolejnym problemem związanym z utratą danych jest możliwość ich odzyskiwania. Jeśli chodzi o szacunkową ilość danych odzyskiwanych (badania przeprowadzone przez firmę Ontrack Data Recovery) w latach 2002 i 2010, można stwierdzić, że nastąpiła również zmiana poszczególnych rodzajów przyczyn. W roku 2010 w porównaniu z 2002 największe pozytywne zmiany zaszły w przypadku odzyskiwania danych utraconych w wyniku działania wirusów komputerowych (1,75 razy). Wnioskować z tego można, że nastąpił istotny wzrost poziomu jakościowego oprogramowania antywirusowego.

Wysoki i pozytywny jest również wskaźnik dynamiki (1,5) odzyskiwania danych utraconych w wyniku klęsk żywiołowych, jednak jego znaczenie w całości

przyczyn utraty danych nie jest istotne ze względu na niski udział tej przyczyny we wszystkich czterech rodzajach przyczyn utraty danych.

Negatywny wzrost wykazują głównie dwie przyczyny odzyskiwania utraconych danych, a mianowicie: sprzęt komputerowy i błędy w oprogramowaniu. W przypadku wystąpienia błędu wynikającego z problemów sprzętowych możliwość odzyskiwania danych w 2010 roku kształtowała się na poziomie tylko 29% i była gorsza niż w roku 2002, kiedy wskaźnik ten wynosił 56%. Natomiast jeśli chodzi o przyczynę określaną jako błędy w oprogramowaniu, to możliwość odzyskiwania danych w 2010 roku wynosiła 7%, a w 2002 − 9%.

Podsumowując, należy wskazać, że najmniejsze zmiany (1,04) wykazuje wskaźnik dynamiki odzyskiwania danych spowodowany błędem człowieka. W kontekście zaprezentowanych danych w tabeli 1 można więc potraktować go jako stały, choć także negatywny, wśród wszystkich wymienianych przyczyn utraty danych.

W dalszej części opracowania rozważania zostaną ograniczone do omówienia zagrożeń dla systemów informatycznych wynikających ze świadomego bądź nieświadomego działania człowieka.

3. Człowiek źródłem zagrożeń w procesie tworzenia i funkcjonowania systemu informatycznego

Zasoby ludzkie stanowią jeden z ważniejszych i silnie oddziałujących elementów na systemy informatyczne. Zagrożenia osobowe dotyczą przede wszystkim procesu tworzenia systemów informatycznych, włamań do baz danych systemu, podsłuchu, niszczenia danych, wprowadzania wirusów, a także zaniedbywania obowiązków przez pracowników. Zagrożenia te mogą pochodzić zarówno z przedsiębiorstwa, jak i jego otoczenia. Gros zagrożeń powstaje na etapie tworzenia systemu informacyjnego.

W procesie tworzenia systemu informatycznego zagrożenia wynikające z zasobów ludzkich mogą być spowodowane między innymi przez [Stokłosa, Bilski, Pankowski 2001, s. 95]:

- zarząd,
- kierownika projektu,
- zespół projektowy,
- pozostałą część kadry.

Najczęstszym problemem jest brak lub połowiczne zaangażowanie zarządu w cały proces. Nie wystarcza sama wola zmiany, muszą za tym iść konkretne działania. Oczywiście nie chodzi tu o angażowanie się w procesy operacyjne, jednak każdy pracownik musi czuć, że projekt ten to przysłowiowe „oczko w głowie zarządu". Dużym niebezpieczeństwem jest też zmiana priorytetów firmy w trakcie trwania projektu. Powoduje to często rozwlekanie wdrożenia w czasie, co może skutkować znacznym obniżeniem jakości wprowadzanego systemu.

Innym zagrożeniem może być zmiana własnościowa w firmie (jeden z częstych przypadków przerwania projektu nawet przy dużym zaangażowaniu kapitałowym).

Bardzo często zmiana własnościowa wymusza zmianę zarządu firmy. Nowy zarząd w wielu przypadkach rezygnuje z kontynuowania zadań rozpoczętych przez swoich poprzedników. Konsekwencją takiego postępowania jest znaczne zwiększenie kosztów informatyzacji albo zaniechanie prowadzonych prac

Częstym błędem jest też niewłaściwe umocowanie kierownika projektu. Może to być poważną przeszkodą w sprawnym przeprowadzeniu wdrożenia i zwykle prowadzi do konfliktów interpersonalnych związanych z brakiem określenia kompetencji dla poszczególnych pracowników, a w wielu przypadkach brakiem kompetencji w ogóle. Powierzenie wdrożenia niedoświadczonemu kierownikowi stanowi źródło wielu zagrożeń. Niedoświadczony kierownik często niewłaściwie zarządza pracami wdrożeniowymi. Przykładem może być jedno z dużych przedsiębiorstw we Wrocławiu, w którym na tak poważne stanowisko, kierownika projektu, powołano osobę pracującą dość długo w przedsiębiorstwie, ale nieznającą się na rzeczy (tworzenia i wdrażania systemów informatycznych), zamiast zatrudnić specjalistę z zewnątrz. Działanie to miało na celu obniżenie kosztów wdrożenia. Osoba ta miała kierować całym zespołem wdrożeniowym. Nie mając praktycznie żadnego doświadczenia w tej dziedzinie, podjęła kilka decyzji sprzecznych i wzajemnie się wykluczających. W efekcie doszło do rozbicia zespołu wdrożeniowego, nie było osób odpowiedzialnych za prowadzenie określonych etapów prac, założenia wdrożenia zostały błędnie zdefiniowane i w wkrótce należało utworzyć nowy zespół. Podrożyło to znacznie koszty i wydłużyło prawie o rok prace wdrożeniowe.

W celu zmniejszenia wpływu błędów na realizację całościową projektu należy odpowiednio wprowadzić mechanizmy ich śledzenia [Pietruszewski 2006, s. 136]:

– sposób raportowania o błędzie,
– procedury identyfikacji (potwierdzania) błędu oraz przydzielania go do różnych kategorii,
– klasy priorytetów odnoszące się do wymagań dotyczących czasu likwidacji błędu,
– zasady przydzielania błędu do likwidacji określonej grupie,
– sposoby weryfikacji rozwiązania błędu.

Kolejnym poważnym źródłem zagrożeń jest zła motywacja kierownika projektu lub jej całkowity brak. Należy pamiętać, że jest to osoba najważniejsza dla powodzenia projektu. Zwykle oddelegowana w pełni do przeprowadzenia wdrożenia obawia się o swoją przyszłość (typowe obawy: co po wdrożeniu, nie mam do czego wracać, moje miejsce jest zajęte). Dlatego niedopuszczalne jest pominięcie aspektu motywacji w pełnym tego słowa znaczeniu, czyli niezapewnienie dalszego ciągu pracy. Założenie, że dodatek zadaniowy (premia zadaniowa) wszystko załatwi, jest błędne.

Zespół projektowy to kolejne źródło zagrożenia ze strony zasobów ludzkich na etapie tworzenia systemu informatycznego. Ważnym elementem jest zdiagnozowanie, czy powołany zespół ma wiedzę merytoryczną oraz umiejętności współpracy grupowej. Częstymi zagrożeniami są na przykład:

– niewłaściwe kompetencje lub ich brak,
– nieodpowiednie cechy osobowe,
– brak umiejętności pracy zespołowej,
– brak odporności na stres.

Po takiej analizie, gdy występują wspomniane zagrożenia, możemy przebudować zespół, ale życie pokazuje, że trudno stworzyć ideał. Dlatego najważniejszym zadaniem jest zdiagnozowanie wszystkich słabych punktów zespołu, tak aby w przyszłości ograniczyć ryzyko poprzez przedsięwzięcie odpowiednich działań w procesie doboru członków zespołu. Aby zmniejszyć ten typ zagrożenia, wskazane jest uwzględnienie następujących warunków, mających na celu maksymalizowanie wartości dzielenia się przez członków zespołu wiedzą [Perechuda, Sobińska 2010, s. 397]:

– pracownicy powinni zrozumieć, jakie korzyści daje im dzielenie się wiedzą,
– pracownicy powinni wiedzieć, jakie korzyści proces ten daje całej organizacji,
– zarządzający muszą uznawać i cenić dzielenie się wiedzą,
– dzielenie się wiedzą powinno stać się integralną częścią codziennej pracy ludzi,
– powinien istnieć system wynagradzania i wyróżniania ludzi, mający na celu promowanie tych pracowników, którzy przystosowali się do nowych zachowań.

Kolejnym istotnym obszarem jest motywowanie zespołu. Tworząc regulamin motywacyjny, trzeba przeciwdziałać takim zagrożeniom, jak: brak identyfikacji z celami projektu. Paraliżujący strach przed brakiem możliwości powrotu na poprzednie stanowisko jest jeszcze silniejszy niż w przypadku kierownika. Jest to także bardzo często strach przed alienacją z zespołu, z całej załogi. Często w parze z niewłaściwym umocowaniem kierownika idzie brak określenia uprawnień zespołu, sprzyjają temu szczególnie niejasne reguły podległości służbowej[3].

Inną grupę zagrożeń ze strony zasobów ludzkich w zakresie prac związanych z procesem tworzenia systemu informatycznego stanowi pozostała część załogi będąca w przyszłości użytkownikami systemu. Ze względu na to, że pozostała część załogi staje się niejako biernym uczestnikiem projektu, to największym zagrożeniem jest niezrozumienie celów projektu. Skutkuje to często całkowitym brakiem motywacji do wdrożenia projektu w firmie, a nawet jego bojkotowaniem. Występuje tu szereg typowych ludzkich obaw przed zmianą, które stają się potencjalnym zagrożeniem dla wdrożenia projektu. Najczęstsze to poczucie zagrożenia dotychczasowej pozycji oraz obawa przed redukcją miejsc pracy.

Kolejnym zagrożeniem, choć może się to wydać paradoksalne, jest chęć wykazania się własnymi pomysłami. Osoby niemające zwykle pełnego obrazu sytuacji mogą sugerować rozwiązania rozbieżne z celami projektu, nieuwzględniające celów istotnych dla przedsiębiorstwa. Po odrzuceniu ich pomysłów czują się ignorowani i w wielu przypadkach zaczynają wręcz przeszkadzać w procesie wdrażania projektu.

---

[3] Szerzej problemy zarządzania projektami i związane z nimi konflikty osobowe rozpatruje J. Brilman [2002].

Ostatnią grupę stanowią tzw. zagrożenia pozostałe. Do nich należy zaliczyć między innymi niewłaściwe umiejscowienie projektu wdrożeniowego w strukturze firmy. Taka niewłaściwa lokalizacja projektu wdrożeniowego może wyzwalać problemy z określeniem kompetencji i uprawnień poszczególnych pracowników oraz kierownika odpowiedzialnego za prowadzony projekt. Inną barierą trudną do pokonania jest bariera finansowa związana z zatrudnieniem specjalistów wdrażających system. Dlatego też coraz częściej firmy odchodzą od zatrudniania pracowników na umowę o pracę na rzecz tzw. samozatrudnienia.

Problematykę zagrożeń systemów informatycznych w procesie jego tworzenia przedstawiono w pracy [Zając]. Opisywane są tam zagadnienia związane z konfliktami na etapie prac projektowo-wdrożeniowych

Ze względu na wpływ konfliktu na powodzenie projektu i możliwość przeciwdziałania lub sterowania nim, można wyodrębnić cztery możliwe sytuacje [Zając]:

1) istnienie konfliktu w organizacji jeszcze przed przystąpieniem do realizacji projektu,

2) powstanie konfliktu w trakcie prac nad nowym SI,

3) powstanie konfliktu w efekcie wprowadzenia nowego SI,

4) zaistnienie konfliktu w zespole projektowym.

Rozpatrując pierwszą sytuację, tj. istnienie konfliktu, należy dążyć do poznania przyczyn konfliktu oraz dokonać próby jego neutralizacji. Analiza czynników konfliktogennych może doprowadzić do uzyskania odpowiedzi na pytanie, czy i w jakim stopniu zastosowanie technologii informacyjnych może pozwolić sterować konfliktem bądź zminimalizować jego negatywne oddziaływanie. Do zadań kierownika zespołu projektowego należy identyfikacja osób zamieszanych w konflikt i odpowiednie nimi pokierowanie lub w ostateczności wyeliminowanie niektórych z nich. Rozwiązanie takie może oczyścić atmosferę grupy pracowniczej, która będzie przynależeć w przyszłości do zespołu projektowego. Groźne może to być w sytuacji, gdy poszczególni pracownicy będą udzielać informacji członkom zespołu projektowego. W trakcie tego procesu mogą pojawiać się problemy związane z rzetelnym przekazywaniem informacji do celów analizy systemu informatycznego, badania potrzeb informacyjnych, a później już na etapie projektowania systemu informatycznego.

W przypadku powstania konfliktu w trakcie prac nad nowym systemem informatycznym należy dążyć do realizacji potrzeb informacyjnych przyszłych użytkowników, gdyż to oni najczęściej są poszkodowani na skutek zmian organizacyjnych, zakresów nowych obowiązków. Pamiętać trzeba, że w trakcie projektowania systemu określa się dość często nowe procedury przetwarzania danych, w znacznym stopniu automatyzuje się czynności prac biurowych, a to skutkuje zmniejszonym zapotrzebowaniem na siłę roboczą. Jednak uwzględniając te zagrożenia, celowe jest zwracanie uwagi na efektywność proponowanych zmian, które znajdą odzwierciedlenie w systemie informatycznym. Unikanie w tym procesie konfliktów pozwoli prawidłowo zaprojektować przyszły system.

W trzeciej sytuacji rozpatruje się powstanie konfliktu w efekcie wprowadzenia nowego systemu. Występuje ona najczęściej w przypadku zakupienia gotowego nowego systemu bez przeprowadzenia gruntownej analizy potrzeb informacyjnych i dostosowania procedur programowych do specyfiki przedsiębiorstwa. Pokreślić należy, że oprogramowanie dostępne na rynku często nie spełnia wymagań stawianych przez użytkowników. W pewnym stopniu tej sytuacji konfliktowej można uniknąć, prawidłowo dobierając system na rynku z dużymi realnymi możliwościami parametryzacji procedur przetwarzania danych. Ponadto wskazane jest włączanie przyszłych użytkowników w proces adaptacji systemu do konkretnych potrzeb przedsiębiorstwa. Wyzwala to pozytywne reakcje tych użytkowników i powoduje większe zaangażowanie w proces wprowadzania systemu.

Ostatnią omawianą sytuacją jest zaistnienie konfliktu w zespole projektowym. Prawidłowo zorganizowany i dobrany zespół projektowy składa się z przedstawicieli kierownictwa przedsiębiorstwa (tzw. decydentów), analityków systemu, projektantów, programistów, wyselekcjonowanych użytkowników końcowych (tzw. użytkownicy twórcy). Każdy z uczestników tego zespołu postrzega system ze swojego punktu widzenia i forsuje swoje rozwiązania, co wywołuje konflikt. Zadaniem kierownika zespołu jest takie sterowanie nim, żeby można było zrealizować projekt zgodny z zamierzonymi celami, przy określonych kosztach i w określonym terminie. Zalecane podejście do sterowania konfliktem między poszczególnymi grupami zespołu projektowego przedstawia tabela 2.

Tabela 2. Zalecane podejście do konfliktu między grupami uczestników procesu tworzenia systemu

Uczestnicy zespołu projektowego	Decydenci	Analitycy	Użytkownicy bezpośredni	Użytkownicy twórcy
Decydenci	u	u	u	u
Analitycy	u	s	u	s
Użytkownicy bezpośredni	u	u	s	s
Użytkownicy twórcy	u	s	s	s

u – unikać, s – sterować

Źródło: [Zając].

Innym problemem jest specyfika wykonywania przyszłej pracy. Ci ludzie przyzwyczajeni do trudów wdrożenia, frustrują się codzienną monotonią pracy. Jeżeli firmie zależy na ich utrzymaniu, musi mieć plan, co może im w przyszłości zaoferować po całkowitym wdrożeniu systemu.

4. Cechy osobowościowe i profesjonalizm członków zespołu projektowego

Każda organizacja musi się liczyć z zagrożeniami, zarówno zewnętrznymi jak i wewnętrznymi w procesie tworzenia systemu informatycznego. Ważną rolę odgrywają tu zasoby ludzkie. Nawet najlepszy system zawiedzie, gdy ludzie nie będą przestrzegać ustalonych zasad. Aby skutecznie przeciwstawiać się zagrożeniom pojawiającym się w procesie tworzenia systemu informatycznego, organizacja powinna mieć opracowaną politykę eliminacji zagrożeń dostosowaną do swojej specyfiki. Podkreślić należy, że współczesne firmy dążą do zniwelowania zagrożeń w procesie wdrażania systemu informatycznego, których źródłem są zasoby ludzkie. Powinny one podjąć odpowiednie działania już na etapie wdrażania tego systemu. Prawidłowy dobór kadry informatycznej zapewni przedsiębiorstwu właściwy proces tworzenia i funkcjonowania systemów informatycznych. Dlatego też selekcja przy wyborze osób do procesów informatyzacji jest szczególna. Oprócz znajomości zagadnień z zakresu informatyki dużą wagę przywiązuje się do następujących cech:

– Komunikatywność – informatycy muszą często współpracować z użytkownikami końcowymi, którzy zazwyczaj zaangażowani są w pełni w codzienne obowiązki i nie znają procesów tworzenia i funkcjonowania systemów informatycznych. Z tego powodu ci ostatni mają trudności ze zrozumieniem pewnych rozwiązań.
– Umiejętność pracy w zespole − występują tu pewne trudności, gdyż najlepsi informatycy są zazwyczaj indywidualistami, a to powoduje napięcia i konflikty w procesie tworzenia systemu i jego wdrażania. Silne cechy osobowościowe poszczególnych członków zespołu mogą utrudniać realizację projekt z tego względu, że każdy z nich chce przeforsować swoje pomysły, rozwiązania. Pokreślić należy, że niektóre z nich mogą być sprzeczne lub niekompatybilne.
– Znajomość procesów biznesowych w przedsiębiorstwach − informatycy często zajmują się projektowaniem nowych rozwiązań, a nie mają wiedzy merytorycznej w zakresie projektowanego systemu. Aby zmniejszyć ten czynnik, wskazane jest ich pewne przeszkolenie w zakresie prowadzonego biznesu i wymogów w nim obowiązujących. Pozwoli to lepiej zaprojektować system i dostosować go potrzeb organizacji.
– Znajomość języków obcych − ta cecha jest szczególnie istotna w przypadku dużych przedsiębiorstw, gdzie prowadzi się duże projekty, które mają zazwyczaj charakter międzynarodowy. Przykładem może tu być duży koncern międzynarodowy, w którym tworzy się „wirtualne zespoły" do obsługi systemów informatycznych. Członkowie zespołów z różnych krajów dobierani są do nich na podstawie posiadanych umiejętności (np. rachunkowość, logistyka, zarządzanie jakością), dzięki czemu mogą rozwiązywać w określonym zakresie problemy użytkowników z innych krajów. Wejście Polski do Unii Europejskiej powoduje zmiany przepisów prawnych – mamy tu do czynienia ze standaryzacją i unifika-

cją prawa. Standaryzacja i unifikacja wywołują także zmiany w oprogramowaniu systemów informatycznych na skutek reorganizacji procesów biznesowych.

– Odporność na stres − ze względu na duże nakłady finansowe oraz złożoność rozwiązywanych problemów informatycy są szczególnie narażeni na konsekwencje błędnie prowadzonych projektów informatycznych. Należy dodać, że to właśnie przy projektach informatycznych mamy do czynienia z problematyczną wyceną prac informatycznych. Dobry pracownik działu informatyki to konsultant wszechstronny, który ma znajomość zasad programowania, ale też potrafi przygotować poprawne rozwiązania merytoryczne, przeszkolić użytkownika końcowego i samodzielnie poszukiwać nowych rozwiązań w zakresie poprawy jakości wdrożonego systemu informatycznego.

5. Podsumowanie

W procesie tworzenia systemu należy rozpatrzyć kilka kluczowych elementów, które są przedmiotem bądź podmiotem projektowania, a następnie wdrażania. Do tych kluczowych elementów należy zaliczyć: zasoby ludzkie, informacyjne, proceduralne i techniczne. Spośród tych wszystkich zasobów zasadnicze znaczenia, z punktu widzenia sukcesu procesu tworzenia i wdrażania systemu informatycznego, przypisuje się zasobom ludzkim. W świetle badań prowadzonych przez firmę Ontrack Data Recovery zasoby ludzkie (czynnik ludzki) są przyczyną dużej liczby błędów. W przypadku utraty danych w systemach informatycznych czynnik ludzki powoduje 40% błędów (dane z roku 2010), a wziąwszy pod uwagę błędy w oprogramowaniu, to łączny udział błędów spowodowanych czynnikiem ludzkim wynosi aż 52%.

Dlatego też należy szczególnie zwrócić uwagę na poszukiwanie rozwiązań mających na celu zmniejszenie udziału błędów ludzkich w szeroko rozumianym działaniu systemów informatycznych. Zmniejszenie to można uzyskać między innymi poprzez odpowiedni dobór cech osobowościowych zespołu projektowego, a w przypadku wdrażania systemu i jego eksploatacji − właściwe szkolenia użytkowników końcowych.

Literatura

Brilman J., *Nowoczesne koncepcje i metody zarządzania*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2002.

Kisielnicki J., Sroka H., *Systemy informacyjne biznesu*, Wydawnictwo Placet, Warszawa 1999.

McNamara J., *Arkana szpiegostwa komputerowego*, Warszawa 2003.

Nowicki A., *Strategia doskonalenia systemu informacyjnego w zarządzaniu przedsiębiorstwem*, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław 1999.

Perechuda K., Sobińska M., *Zarządzanie informacją i wiedzą w outsourcingu IT*, [w:] J. Korczak, I. Chomiak-Orasa, H. Sroka (red.), *Systemy informacyjne w zarządzaniu*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2010.

Pietruszewski W., *Błędy w projektach informatycznych*, [w:] *Ryzyko przedsięwzięć informatycznych. Materiały Ogólnopolskiej Konferencji Naukowej*, Politechnika Szczecińska, Szczecin 2006.

Stokłosa J., Bilski T., Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, Warszawa 2001.

Understanding Data Loss, http://www.ontrackdatarecovery.com/understanding-data-loss/, 14.10.2010.

Utrata danych efektem błędu człowieka http://www.egospodarka.pl/55394,Utrata-danych-efektem-bledu- czlowieka,1,39,1.html. 14.10.2010.

Woda M., *Bezpieczeństwo systemów informatycznych*, http://www.zsi.pwr.wroc.pl/zsi/missi2004/pdf/Woda%20Marek.pdf. 30.09.2010.

Zając A., *Wpływ konfliktu organizacyjnego na powodzenie przedsięwzięć informatycznych*, http://ki.ae.krakow.pl/~zajaca/artykuly/kon_zn96.html. 10.10.2010.

HUMAN FACTOR AS A SOURCE OF THREATS IN THE PROCESS OF CREATING AND FUNCTIONING OF IT SYSTEM IN AN ENTERPRISE

Summary: Human resources are the most important elements of information system. Therefore they can be also an important source of threats during the process of creating as well as functioning of information system. Usually, these threats may appear on every level of creating the information system and may come from both internal and external environment of an enterprise. The article presents the main threats connected with human factor during the process of creating the information system.