PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 119
Informatyka Ekonomiczna 18 2010

Damian Dziembek
Politechnika Częstochowska

CZYNNIKI RYZYKA DOTYCZĄCE UŻYTKOWANIA APLIKACJI W MODELU SAAS

Streszczenie: W efekcie znacznego rozwoju technologii informacyjno-komunikacyjnej oraz konkurencji na rynku IT pojawiają się nowe możliwości zakupu i użytkowania systemów informatycznych przez przedsiębiorstwa. Współcześnie interesującą i dynamicznie rozwijającą się formą dostępu i eksploatacji oprogramowania jako usługi jest model SaaS (*Software as a Service*), w którym podmioty gospodarcze uzyskują możliwość zdalnego użytkowania różnych typów oprogramowania za pośrednictwem sieci internet. W artykule wskazano główne czynniki ryzyka dla modelu SaaS. Identyfikacja czynników ryzyka dla modelu SaaS może wspomóc decydentów rozważających zastosowanie tej formy dystrybucji i użytkowania aplikacji w swych organizacjach.

Słowa kluczowe: model SaaS, e-outsourcing informatyczny, czynniki ryzyka.

1. Wstęp

W wyniku rozwoju technologii informacyjno-komunikacyjnej oraz konkurencji na rynku IT pojawiają się nowe możliwości zakupu i użytkowania systemów informatycznych przez przedsiębiorstwa. Interesującą i dynamicznie rozwijającą się formą dostępu i eksploatacji oprogramowania jako usługi jest model SaaS (*Software as a Service*). W modelu tym podmioty gospodarcze uzyskują możliwość zdalnego użytkowania różnych typów oprogramowania za pośrednictwem internetu.

Model SaaS jest stosunkową nową formą eksploatacji oprogramowania przez przedsiębiorstwa. Celem artykułu jest prezentacja głównych czynników ryzyka związanych z modelem SaaS. Różnorodne czynniki ryzyka zostały zidentyfikowane na podstawie kilku kryteriów, których analiza może być przydatna przy podejmowaniu decyzji o rozpoczęciu użytkowania aplikacji w modelu SaaS.

2. Identyfikacja czynników ryzyka dla modelu SaaS

Według firmy IBM – SaaS to dynamicznie rozwijany model biznesowy, wpływający na rynek dostawców oprogramowania, w którym aplikacja (wraz z jej funkcjonalnością) jest dostarczana odbiorcom przez Internet w formie subskrypcji. Klienci nie przejmują na własność oprogramowania, lecz zdalnie dzierżawią kompletne rozwiązania informatyczne zaoferowane przez dostawców zainteresowanych zwiększaniem swego udziału w rynku IT [IBM: SaaS…].

Rozważając zastosowanie modelu SaaS, klient powinien być świadomy ryzyka związanego ze zdalną eksploatacją oprogramowania. Oczywiście ryzyko stanowi nieodłączny element jakiejkolwiek działalności człowieka (w tym realizacji różnorodnych przedsięwzięć gospodarczych). Ogólnie ryzyko można określić jako możliwość wystąpienia niepożądanych zdarzeń, mających lub mogących mieć wpływ na osiągnięcie celu założonego przy podejmowaniu określonej decyzji. Ryzyko definiuje się także jako niebezpieczeństwo poniesienia straty (lub uzyskanie mniejszego niż oczekiwano poziomu dochodów) (por. [Sierpińska, Jachna 1999].

Ważnym elementem działań zmierzających do redukcji ryzyka jest wytypowanie czynników wpływających na prawdopodobieństwo wystąpienia negatywnych zdarzeń, utrudniających osiągnięcie zakładanego celu (tzw. identyfikacja czynników ryzyka). Identyfikacja czynników ryzyka modelu SaaS jest pierwszym etapem wchodzącym w skład kompleksowego zarządzania ryzykiem dotyczącego e-outsourcingu informatycznego (obejmującego ponadto ocenę, monitorowanie ryzyka oraz zapobieganie mu) (por. [Szyjewski 2004]).

Źródłem ryzyka w przypadku modelu SaaS są różnorodne czynniki o charakterze negatywnym, które wpływają (lub mogą wpływać) na jego skuteczność, parametry oraz wyniki ekonomiczne. W tab. 1 (na bazie studiów literaturowych) przedstawiono różne czynniki ryzyka charakterystyczne dla modelu SaaS, ujęte z punktu widzenia klienta (odbiorcy). W celu uniknięcia powtórzeń w dalszych rozważaniach będą używane zamiennie terminy SaaS oraz e-outsourcing informatyczny.

Czynniki ryzyka związane z zastosowaniem modelu SaaS mogą być w różnorodny sposób systematyzowane. Głównym kryterium podziału czynników ryzyka może być źródło jego pochodzenia, tj. (por. [Dziembek 2009]):

1. Miejsce powstania – w tym przypadku czynniki ryzyka można pogrupować na zewnętrzne (dotyczące otoczenia dostawcy i klienta) oraz wewnętrzne (odnoszące się do zawartej umowy dotyczącej użytkowania aplikacji w formie SaaS).

2. Czynniki ryzyka o charakterze zewnętrznym determinują funkcjonowanie zarówno dostawcy, jak i odbiorcy aplikacji w modelu SaaS na rynku. Wspomniane czynniki (np. trendy rozwoju rynku IT, niekorzystne zmiany polityczne) wpływają na możliwości rozwoju działalności e-outsourcingowej na rynku IT oraz oddziałują na postrzeganie modelu SaaS przez istniejących oraz potencjalnych odbiorców.

Tabela 1. Czynniki ryzyka użytkowania aplikacji w modelu SaaS

Kryterium podziału źródeł ryzyka	Czynniki ryzyka	Przykłady czynników ryzyka
1	2	3
Miejsce powstania	Zewnętrzne	Wzrost inflacji, trendy rozwoju rynku IT, zmiany polityczne, recesja na rynku IT itp.
	Wewnętrzne	Wybór niewłaściwego dostawcy i oprogramowania SaaS, nierealne oczekiwania odbiorcy co do jakości usług, złe zarządzanie współpracą po stronie dostawcy i/lub odbiorcy, brak odpowiednich zasobów dostawcy SaaS itp.
Sfera powstawania	Makroekonomiczne	Recesja gospodarcza, wzrost inflacji, niestabilność polityczno-prawna (nieoczekiwane zmiany aktów prawnych), wzrost obciążeń podatkowych, niekorzystna zmiana kursów walutowych, zawieszenie ulg inwestycyjnych, brak polityki w zakresie dofinansowania innowacyjnych projektów itp.
	Mikroekonomiczne	Mała liczba dostawców SaaS na rynku, recesja na rynku IT, niewystarczające zasoby do świadczenia e-usług po stronie dostawcy, częste awarie w świadczeniu usług – zależne i niezależne od dostawcy SaaS, wahania jakości w użytkowaniu SaaS, brak wzorców postępowania, nieuprawniony dostęp innych podmiotów do danych odbiorcy SaaS itp.
	Pozaekonomiczne	Kataklizmy, powódź, pożar, zamieszki zbrojne, ataki terrorystyczne itp.
Obszar	Organizacyjno-zarządcze	Błędny wybór dostawcy SaaS, przyjęcie niekorzystnych zapisów umowy SLA przez odbiorcę (w tym podpisanie umowy SLA zawierającej błędy prawne lub niewłaściwie zabezpieczającej interesy klienta), brak odpowiedniego lidera projektu po stronie odbiorcy lub nagła utrata personelu sterującego pracami w zakresie implementacji SaaS, utrata kontroli odbiorcy nad zgromadzonymi danymi, słabe zaangażowanie naczelnego kierownictwa w pracach wdrożeniowych SaaS (szczególnie aplikacji o strategicznym znaczeniu), brak analizy dotyczącej efektywności zastosowania SaaS itp.
	Techniczno-technologiczne	Niedopasowanie technologii do potrzeb i oczekiwań odbiorcy, nieodpowiedni poziom wiedzy technicznej personelu dostawcy SaaS, niższa od zakładanej jakość świadczonych usług, niewłaściwe zarządzanie kwestiami technologicznymi w obszarze SaaS (błędna aktualizacja nowych wersji aplikacji SaaS, błędy w migracji danych, błędy administratora itd.), gorsza wydajność od systemów eksploatowanych w formie tradycyjnej, brak możliwości integracji z innymi aplikacjami, wyciek danych na skutek nieodpowiednich zabezpieczeń, przerwy i awarie utrudniające korzystanie z SaaS, słaba elastyczność w zakresie dopasowania aplikacji do szybkich zmian i potrzeb występujących u odbiorcy SaaS itp.
	Rynkowo-branżowe	Zmniejszanie popytu/podaży usług SaaS, niekorzystne trendy lub wydarzenia na rynku IT obniżające zaufanie do modelu SaaS, brak odpowiednich zasobów u dostawców gwarantujących wysoki poziom świadczonych usług SaaS na rynku, utrata płynności oraz bankructwo dostawcy SaaS, bariery komunikacyjne, zawirowania na rynku IT wpływające na cenę/jakość SaaS, brak ubezpieczeń od ryzyk związanych z SaaS itp.
	Prawno-polityczne	Polityka rządu wpływająca na wzrost kosztów, możliwość konfliktu międzynarodowego, niestabilność prawa (tworzenie dodatkowych licencji, koncesji i zezwoleń), trudności w zakresie roszczeń odszkodowawczych (problem jurysdykcji odnośnie do SaaS, różne regulacje prawne w krajach dostawcy i odbiorcy), niekorzystne zmiany kursów walutowych, wzrost inflacji, wzrost podatków itp.
	Pozostałe (sił wyższych)	Wystąpienie nieoczekiwanych zdarzeń losowych, np. pożar, powódź, trzęsienie ziemi, konflikty zbrojne, ataki terrorystyczne itp.

Tabela 1, cd.

1	2	3
Faza umowy outsourcingowej	Przed transakcją	Błędne oszacowanie kosztów IT po stronie odbiorcy, niewłaściwa specyfikacja potrzeb, złe zapytanie ofertowe, brak sformułowanych celów dla SaaS, brak kompleksowego planu wdrożenia SaaS u odbiorcy, posiadanie niepełnej informacji co do specyfiki usług SaaS, błędny wybór dostawcy SaaS, brak lub niewłaściwy dobór osób do zarządzania implementacją SaaS, nadanie niskiego priorytetu dla projektu SaaS względem innych przedsięwzięć realizowanych u odbiorcy, brak analizy dostawcy pod względem kosztu, jakości, zabezpieczeń itp.
	Związane z transakcją	Przyjęcie nierealnego harmonogramu w zakresie wdrożenia SaaS, akceptacja zbyt wysokich kosztów SaaS, przyjęcie zbyt niskiej jakości usług SaaS, przyjęcie niekorzystnej umowy SLA, brak odpowiednich zabezpieczeń prawnych dla odbiorcy SaaS, brak motywacji lidera projektu po stronie odbiorcy, realizacja również innych złożonych projektów w tym samym czasie (rozpraszanie czasu, energii, zasobów), złe zabezpieczenie umowy SLA pod względem inflacji, zmian kursów walut itp.
	Po transakcji	Brak spodziewanej obniżki kosztów, niespełnienie wymogów jakościowych przez dostawcę SaaS (nieprzestrzeganie parametrów zdefiniowanych w SLA), trudności w rozwiązywaniu typowych oraz nietypowych problemów na linii odbiorca-dostawca, pogarszanie jakości współpracy dostawca-odbiorca, konflikty skutkujące nawet rozstrzygnięciami sądowymi, załamania na rynku IT, pojawianie się wad ukrytych w stosowanych aplikacjach oferowanych jako SaaS, niewłaściwy system zabezpieczeń dostawcy SaaS skutkujący wyciekiem danych odbiorcy, nagła likwidacja działalności przez dostawcę SaaS, nagłe i częste awarie oraz brak szybkich reakcji ze strony dostawcy SaaS skutkujące brakiem ciągłości produkcji/sprzedaży, wzrost stóp procentowych, kursu walut, podatków lub inflacji zwiększających koszty SaaS, działania siły wyższej (kataklizmy, wojny itp.), zmiany w technologii wymuszające nowe inwestycje, wzrost kosztów eksploatacji, mała elastyczność dostawcy SaaS do pojawiających się potrzeb dostawcy lub długi czas wprowadzania nowych modyfikacji, zawyżanie kosztów w zakresie dodatkowych usług, konflikt interesów projektu z innymi projektami realizowanymi w firmie, brak planu awaryjnego na wypadek zakończenia działalności przez dostawcę SaaS itp.
Kluczowe elementy umowy SaaS	Dostawca	Podawanie przez dostawcę niepełnych lub nieprawdziwych danych co do swoich kompetencji, jakości posiadanych zasobów, standingu finansowego, brak doświadczenia dostawcy w obszarze SaaS, duża liczba jednoczesnych incydentów wpływająca na obniżenie u dostawcy jakości usług SaaS, niska elastyczność dostawcy SaaS do potrzeb odbiorcy, utrata kluczowego personelu przez dostawcę, zawirowania na rynku IT skutkujące obniżką jakości lub zakończeniem świadczenia usług w modelu SaaS, zawyżanie kosztów dodatkowych usług nieobjętych SaaS itp.
	Odbiorca	Przekonanie o braku celowości zastosowania SaaS, brak personelu zdolnego do zarządzania implementacją SaaS, nieznajomość specyfiki SaaS, błędy lub brak oszacowania kosztów TCO, generowanie wyższych kosztów i/lub niższej jakości SaaS w stosunku do własnych zasobów IT (przeprowadzenie błędnej analizy), brak monitorowania kluczowych parametrów usług SaaS, brak nadawania odpowiedniej rangi przez kierownictwo strategiczne dla nowych projektów typu SaaS, brak strategii IT, niezadowolenie klientów odbiorcy z poziomu procesów gospodarczych po implementacji SaaS itp.
	Transakcja	Brak sprecyzowanych celów SaaS, brak planu w zakresie realizacji SaaS, przyjęcie nierealnego harmonogramu implementacji SaaS, niekompletna lub niewłaściwa umowa SLA (niekorzystne zapisy w umowie pod względem kosztów, jakości usług, zabezpieczeń, inflacji, itd.,), różnica co do pojmowania jakości usług przez dostawcę i odbiorcę SaaS (brak precyzyjnych zapisów SLA), trudności w zmianie zapisów umowy SLA i problematyczność rezygnacji z aplikacji oferowanych w modelu SaaS, trudności w zakresie powrotu do insourcingu czy zmiany dostawcy SaaS itp.

Źródło: opracowanie własne.

Wewnętrzne czynniki ryzyka odnoszą się bezpośrednio do współpracy między dostawcą i odbiorcą aplikacji w modelu SaaS (np. niewłaściwy wybór oprogramowania, słaba elastyczność dostawcy itp.) i dotyczą różnych obszarów zarządzania umową o świadczenie e-outsourcingu informatycznego.

2. Sfera powstania – wyróżniono czynniki ryzyka o charakterze makroekonomicznym (obejmujące zjawiska polityczne, społeczne, gospodarcze, prawne i rozpatrywane w skali globalnej), mikroekonomicznym (odnoszące się do rynku usług outsourcingowych i współpracy dostawcy i odbiorcy w ramach modelu SaaS) oraz pozaekonomicznym (głównie natury losowej).

Czynniki makroekonomiczne w różnym stopniu wpływają na przedsiębiorstwa i realizowaną przez nich współpracę outsourcingową. Mogą one dotyczyć głównie niebezpieczeństwa niekorzystnych zmian wartości instrumentów rynkowych w przyszłości (np. stopy procentowej, inflacji) oraz zagrożenia powstania dekoniunktury na rynkach.

Czynniki mikroekonomiczne obejmują różnorodne aspekty związane z niekorzystnymi zjawiskami na rynku IT, odnoszą się do specyfiki współpracy dostawców i odbiorców w modelu SaaS oraz dotyczą zarządzania pojedynczą umową e-outsourcingu informatycznego.

Czynniki pozaekonomiczne (losowe) mogą być od człowieka niezależne (np. trzęsienie ziemi, powódź, wichura, uderzenie pioruna) lub zależne (np. zamieszki zbrojne, strajki, sabotaż). Jeżeli wspomniane czynniki swym zasięgiem obejmą miejsce, w którym dostawca SaaS świadczy swe e-usługi, lub lokalizację odbiorcy, to ich skutki mogą mieć krytyczne znaczenie dla dalszego i skutecznego korzystania z modelu SaaS.

3. Obszar – w tym przypadku czynniki ryzyka podzielono na: organizacyjno-zarządcze (dotyczące kwestii sterowania umową e-outsourcingu IT), techniczno-technologiczne (związane z doborem oraz eksploatacją różnorodnych środków oraz narzędzi sprzętowych i programowych), rynkowo-branżowe (odnoszone do zachowania dostawcy/dostawców modelu SaaS), prawno-polityczne (dotyczące zjawisk gospodarczych występujących w danym kraju, działalnością rządu, funkcjonowaniem instytucji państwowych, itp.) oraz pozostałe (związane z działaniem sił wyższych).

4. Czynniki ryzyka o charakterze organizacyjno-zarządczym dotyczą działań lub zaniechań osób po stronie dostawcy usług SaaS oraz odbiorcy, jak również odnoszą się do składu i kompetencji zespołów powołanych do sterowania współpracą w ramach e-outsourcingu IT. Brak profesjonalizmu dostawcy/odbiorcy, niedbałość czy brak wiedzy w zakresie zarządzania współpracą e-outsourcingową znacznie zwiększają ryzyko SaaS. Szczególnie brak celu, zła ocena potrzeb w zakresie IT, niewłaściwe rozpoznanie realnych możliwości dostawcy w zakresie jakości e-usług IT, brak kontroli nad działaniami dostawcy SaaS mogą wpłynąć na poważne zagrożenie osiągnięcia korzyści zakładanych wraz z implementacją e-outsourcingu informatycznego.

Czynniki ryzyka o charakterze techniczno-technologicznym dotyczą głównie niewłaściwej selekcji technologii lub dostosowania jej parametrów do potrzeb odbiorcy. W ramach czynników techniczno-technologicznych mieszczą się również umiejętności i kwalifikacje personelu bezpośrednio związanego z obsługą technologii teleinformatycznych oraz osób odpowiedzialnych za planowanie, organizowanie, koordynację i kontrolę narzędzi i środków IT. Zaoferowanie przez dostawcę nowych, nie do końca sprawdzonych technologii zwiększa ryzyko modelu SaaS. Nowa i nietestowana czy źle dobrana technologia teleinformatyczna u dostawcy SaaS może generować awarie i związane z tym spadki jakościowe, braki dostępności, a także trudności w integracji oraz procesach utrzymania i konserwacji.

Rynkowo-branżowe czynniki ryzyka związane są z bieżącym oraz znacznie bardziej z przyszłym funkcjonowaniem dostawcy (dostawców) oprogramowania w modelu SaaS. Na skutek pojawienia się negatywnych zjawisk na rynku IT mogą nastąpić trudności w dalszej realizacji świadczenia e-usług przez dostawcę (np. wzrost kosztów czy spadek oferowanej jakości usług), a nawet jego bankructwo. Ponadto w początkowym okresie działalności nowi dostawcy oferujący rozwiązania w modelu SaaS mogą dysponować niższą jakością zasobów IT (np. niedoświadczony personel), co może zaniżać parametry jakościowe świadczonych e-usług.

Czynniki prawno-polityczne mogą mieć zasięg krajowy, kontynentalny lub globalny. Nagłe zmiany o charakterze prawno-politycznym (np. wzrost opodatkowania, niekorzystne zmiany prawne dla świadczenia modelu SaaS, zwiększenie kosztów pracy itp.) mogą skutkować trudnościami w realizacji usług e-outsourcingu IT, a nawet zakończeniem działalności dostawcy. Czynniki prawno-polityczne mają szczególne znaczenie, gdy odbiorca analizuje zagranicznego dostawcę SaaS. Specyfika kraju, w którym dostawca oferuje oprogramowanie w modelu SaaS, może odbiegać od standardów stosowanych w kraju odbiorcy.

Czynniki pozostałe dotyczą innych zjawisk i zdarzeń, których nie można zaliczyć do czynników organizacyjno-zarządczych, techniczno-technologicznych, rynkowo-branżowych czy prawno-politycznych. Są one związane z działaniem różnorodnych zjawisk określanych jako siły wyższe (np. pożary, powodzie, trzęsienia ziemi, wyładowania atmosferyczne, strajki generalne, zamachy terrorystyczne, konflikty zbrojne). Czynniki te mają zazwyczaj wpływ na ogół przedsięwzięć realizowanych na danym obszarze terytorialnym (w tym również dotyczą świadczenia usług e-outsourcingu informatycznego).

4. Faza umowy outsourcingowej – według tego kryterium czynniki ryzyka pogrupowano na: występujące przed rozpoczęciem korzystania z oprogramowania w ramach SaaS (poprzedzające fazę podpisania umowy e-outsourcingu informatycznego), związane z umową między dostawcą oprogramowania w modelu SaaS a odbiorcą (odnoszące się do zawierania umowy e-outsourcingu IT oraz jej zapisów) oraz po podpisaniu umowy na świadczenie usług w ramach SaaS (pojawiające się w trakcie obowiązywania umowy e-outsourcingu IT).

Czynniki występujące przed transakcją dotyczą niewłaściwego lub niepełnego przygotowania się odbiorcy do korzystania z e-outsourcingu IT. Ta grupa czynników obejmuje zagrożenia związane z błędną lub niekompletną oceną możliwości realizacji e-usług przez dostawcę SaaS i przyjęciem niewłaściwych założeń do realizacji e-outsourcingu IT. Akceptacja błędnych założeń przez odbiorcę oraz brak sprecyzowania celów zastosowania SaaS mogą mieć znaczny wpływ na późniejszą całościową ocenę efektów implementacji e-outsourcingu informatycznego. Szczególnie istotny jest dobór kompetentnych osób do organizacji i zarządzania implementacją SaaS u odbiorcy, wybór odpowiednich kryteriów oceny dostawców SaaS oraz odpowiednie podejście kierownictwa szczebla strategicznego do problematyki e-outsourcingu informatycznego.

Czynniki ryzyka związane z umową o świadczenie usług SaaS odnoszą się głównie do niekompletnej lub wadliwej pod względem prawnym umowy e-outsourcingu IT. Ważną rolę odgrywają zapisy w umowie dotyczącej poziomu jakości usług SLA (*Service Level Agreement*) precyzyjnie określające obowiązki dostawcy SaaS, zakres i parametry realizowanych przez niego usług oraz jego zakres odpowiedzialności. Przyjęcie niewłaściwych parametrów usług w modelu SaaS w umowie (np. w wyniku pośpiechu, nieodpowiedniej wiedzy zarządzającego kontraktem po stronie odbiorcy itp.) może skutkować niewłaściwym zabezpieczeniem interesów odbiorcy i ponoszeniem dodatkowych kosztów w przyszłości.

Czynniki ryzyka występujące po zawarciu umowy outsourcingowej dotyczą wszelkich zagrożeń powstałych z chwilą podpisania między odbiorcą a dostawcą umowy dotyczącej eksploatacji oprogramowania w modelu SaaS. W okresie po podpisaniu umowy mogą się pojawić niekorzystne zjawiska nie tylko wpływające na sprawność i skuteczność funkcjonowania obszarów wspomaganych przez oprogramowanie udostępnione w modelu SaaS, ale również oddziałujące na całą działalność odbiorcy. Nieodpowiednie zarządzanie współpracą z dostawcą SaaS (a szczególnie brak monitorowania jego działalności) może skutkować zaniżaniem poziomu usług (np. dłuższym czasem reakcji na zgłoszenia serwisowe) oraz wzrostem kosztów. Ponadto możliwe jest pogorszenie przyszłych relacji dostawca-odbiorca SaaS, co w konsekwencji może spowodować odstąpienie odbiorcy od umowy e-outsourcingu informatycznego i powrót do insourcingu (tj. bazowania na własnych zasobach IT).

5. Kluczowe elementy umowy outsourcingowej – w tym przypadku czynniki ryzyka – można rozpatrywać ze względu na dostawcę SaaS, odbiorcę SaaS oraz względem umowy na świadczenie e-outsourcingu informatycznego.

Czynniki ryzyka charakterystyczne dla dostawcy SaaS zwykle odnoszą się do jego negatywnych zachowań, niewłaściwych działań lub dotyczą nieoczekiwanych okoliczności, w których się znalazł. Ważnym czynnikiem ryzyka w tej grupie jest brak odpowiednich umiejętności dostawcy do świadczenia usług e-outsourcingu informatycznego. W niektórych przypadkach dostawca, chcąc pozyskać zlecenie na

użytkowanie aplikacji w modelu SaaS, wyolbrzymia (przejaskrawia) odbiorcy informacje o swych zasobach ludzkich i kapitałowych lub/i proponuje wyjątkowo korzystne ceny e-outsourcingu IT. Zawarcie kontraktu z takim dostawcą może rodzić w przyszłości duże problemy z odpowiednim poziomem jakości przy zaproponowanym poziomie cen. W efekcie może wzrosnąć poziom kosztów użytkowania aplikacji w ramach SaaS lub następuje pogorszenie współpracy dostawca-odbiorca. W sytuacji, gdy konieczne jest przeprowadzenie nagłej i kompleksowej restrukturyzacji działalności odbiorcy wymagającej nowych rozwiązań informatycznych – dotychczasowy dostawca może nie dysponować ofertą oprogramowania atrakcyjnego pod względem funkcjonalnym oraz cenowo/jakościowym. Możliwa jest również sytuacja, w której dostawca SaaS traci wykwalifikowany personel (np. zwolnienie, nagłe odejście pracownika), który odpowiadał za jakość usług e-outsourcingu informatycznego. Taka sytuacja może doprowadzić do pogorszenia jakości SaaS, sporów i w konsekwencji do przedwczesnego rozwiązania umowy, a nawet do rozstrzygnięć sądowych. Czynnikiem ryzyka może się również okazać groźba wycieku istotnych dla odbiorcy danych (jest to najpoważniejsza wątpliwość podnoszona przez odbiorców SaaS) lub zbyt mała liczba dostawców SaaS na rynku, co w przypadku niezadowolenia z jakości współpracy powoduje trudności w poszukiwaniu alternatywnych podmiotów z branży IT, zdolnych do świadczenia usług e-outsourcingu IT na wymaganym poziomie. Ryzyko wzrasta, gdy dostawca SaaS oferuje wysokiej klasy oprogramowanie silnie związane z realizacją celów strategicznych odbiorcy (występuje silne uzależnienie odbiorcy od dostawcy). Wówczas w razie wystąpienia trudności we współpracy trudno jest zastąpić tegoż dostawcę SaaS innym podmiotem z zachowaniem ciągłości usług i dotychczasowych parametrów kosztowo-jakościowych.

Ryzyko niewłaściwego wyboru dostawcy SaaS może się zwiększać na skutek braku kompleksowych informacji dotyczącej jego charakterystyki (tj. sukcesów, porażek, wiedzy i umiejętności dostawcy SaaS). Pomimo poniesienia przez odbiorcę SaaS wstępnych kosztów (koszty poszukiwania, rozmów, selekcji itp.), pełne rozeznanie przez odbiorcę działalności dostawcy jest zadaniem trudnym. Trudności tych świadomy jest dostawca SaaS, który może twierdzić, że posiada niezbędne zasoby i doświadczenie do świadczenia e-outsourcingu informatycznego na wymaganym przez odbiorcę poziomie. W niektórych przypadkach dostawca może przyjąć nadmiernie optymistyczne przeświadczenia co do swoich możliwości w zakresie świadczenia usług SaaS dla odbiorcy oraz liczby przyszłych klientów zainteresowanych jego usługami w przestrzeni wirtualnej. W konsekwencji, po rozpoczęciu udostępniania oprogramowania w modelu SaaS okazuje się, że dostawca nie posiada odpowiedniej liczby klientów lub posiadane rozwiązania technologiczno-organizacyjne nie są wystarczające, w związku z czym nie jest w stanie spełnić oczekiwań odbiorcy pod względem jakości i kosztu usług SaaS. Ponadto dostawca SaaS może nie wypełniać swych zobowiązań, twierdząc że zapisy w umowie SLA

nie są jasne lub pojawiły się okoliczności zaniżające jakość lub zwiększające koszty leżące poza jego kontrolą. Powyższe czynniki mogą skutkować wypowiedzeniem umowy przez odbiorcę i zakończeniem współpracy z dostawcą aplikacji w modelu SaaS.

Czynniki ryzyka charakterystyczne dla odbiorcy wiążą się z zaniechaniem lub podejmowaniem niewłaściwych czynności w ramach użytkowania oprogramowania w modelu SaaS. Kluczowym czynnikiem ryzyka w przypadku odbiorcy jest brak odpowiedniej wiedzy o specyfice modelu SaaS oraz złe i nieskuteczne zarządzanie współpracą z dostawcą e-outsourcingu informatycznego. W efekcie mogą się pojawić błędy związane z niewłaściwym planowaniem eksploatacji aplikacji w przestrzeni wirtualnej, pomyłki i niedopatrzenia w umowie z dostawcą SaaS skutkujące zaniżoną jakością usług oraz trudności w momencie rozwoju lub restrukturyzacji działalności odbiorcy.

Czynniki ryzyka odnoszące się do umowy stanowią różnorodne negatywne zdarzenia związane z zapisami dotyczącymi parametrów e-outsourcingu informatycznego. Oprócz wspomnianych wcześniej błędów umowy e-outsourcingu IT, można wymienić również brak lub nieprecyzyjne ustalenia w zakresie szacowania strat finansowych odbiorcy w przypadku awarii po stronie dostawcy SaaS, niejasne określenie zasad wzrostu kosztów świadczenia e-usług, występowanie (lub brak) możliwości indywidualnych renegocjacji umowy w przyszłości itp.

Gruntowne przeanalizowanie czynników ryzyka związanych z użytkowaniem aplikacji w modelu SaaS ma na celu zdobycie wiedzy przez odbiorcę/klienta o potencjalnych zagrożeniach i stanowi podstawę podjęcia działań zmierzających do ograniczania możliwości ich wystąpienia. Ze wszystkich czynników ryzyka należy wyselekcjonować te z nich, które mogą mieć największy wpływ na powodzenie modelu SaaS, a w kolejnych krokach wskazane jest oszacowanie prawdopodobieństwa ich wystąpienia wraz z poziomem potencjalnych strat, dobór działań zapobiegawczych oraz przeprowadzanie czynności związanych z monitorowaniem ryzyka.

3. Zakończenie

Przedsiębiorstwa użytkujące aplikacje w modelu SaaS powinny być świadome ryzyka związanego z tą bardzo popularną obecnie formą eksploatacji systemu informatycznego. W niniejszym artykule zaprezentowano czynniki ryzyka dla modelu SaaS według różnych kryteriów, co wskazuje na złożoność fazy identyfikacji ryzyka dla tego typu przedsięwzięć. Zamierzeniem autora było zidentyfikowanie najważniejszych czynników ryzyka dla SaaS w celu dostarczenia wiedzy potencjalnym decydentom rozważającym zastosowanie tej formy użytkowania aplikacji. Jakość wykonanych prac w zakresie identyfikacji ryzyka będzie istotnie wpływać na skuteczność dalszych etapów wchodzących w skład zarządzania ryzykiem dla SaaS (tj. na ocenę, monitorowanie ryzyka i zapobieganie mu).

Decyzję o zastosowaniu w przedsiębiorstwie oprogramowania eksploatowanego w ramach modelu SaaS zawsze powinna poprzedzać gruntowna analiza korzyści, kosztów oraz ryzyka związanego z tego typu przedsięwzięciem. Gruntowne przeprowadzenie powyższych czynności pozwoli przedsiębiorstwu we właściwy sposób zarządzać użytkowaniem i rozwojem systemów informatycznych, skutecznie wykorzystywać efekty postępu IT i odnosić sukcesy rynkowe w dynamicznym i zmiennym otoczeniu biznesowym.

Literatura

Dziembek D., *Identyfikacja ryzyka w outsourcingu informatycznym*, [w:] *Zarządzanie ryzykiem w działalności gospodarczej*, red. E. Sitek, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa 2009.

IBM: SaaS, 2007, http://www-304.ibm.com/jct09002c/isv/marketing/saas/index.html.

Sierpińska M., Jachna T., *Ocena przedsiębiorstwa według standardów światowych*, PWN, Warszawa 1999.

Szyjewski Z., *Metodyki zarządzania projektami informatycznymi*, Placet, Warszawa 2004.

RISK FACTORS CONCERNING USAGE OF THE APPLICATION IN THE SAAS MODEL

Summary: New affordabilities and the usage of IT systems in enterprises appear as a result of considerable development of informational communication technology and the competition on the IT market. Nowadays interesting and dynamically developing form of the access and the exploitation of software as service is the SaaS model (Software as a Service) in which economic subjects obtain the possibility of the remote utilization of different types of software via Internet. The article indicates the main risk factors for the SaaS model. The identification of risk factors for the SaaS model can help decision-makers to consider the application of this form of distribution and to use the application in their organizations.