Sylwia Konecka

Ryzyko zakłóceń w przepływie informacji w łańcuchu dostaw

Ekonomiczne Problemy Usług nr 88, 597-604

2012

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 703 EKONOMICZNE PROBLEMY USŁUG NR 88 2012

SYLWIA KONECKA
Wyższa Szkoła Logistyki

RYZYKO ZAKŁÓCEŃ W PRZEPŁYWIE INFORMACJI W ŁAŃCUCHU DOSTAW

Wprowadzenie

Najnowsze badania wskazują, że w jednej na trzy firmy w Wielkiej Brytanii zarządzanie przepływem informacji jest tak ubogie, że przepływ rzeczy jest tak samo szybki albo szybszy. Oszacowano, że straty spowodowane utratą sprzedaży wynikającą z nieefektywności przepływu informacji mogą sięgać w tym kraju nawet 1,2 bilionów funtów rocznie[1]. Przyczyn takiego stanu rzeczy można upatrywać w niedopasowaniu zarządzania przepływem informacji w łańcuchach dostaw do ich funkcjonowania w sferze operacyjnej, niedopasowaniu systemów IT – zaprojektowanych i wdrażanych do zadań realizowanych w obszarze firmy, a nie w sieci dostaw, czy też koncentrowaniu się na przepływie dóbr bez jednoczesnego udoskonalania przepływu informacji w łańcuchu dostaw. Dlatego jednym z istotnych czynników ryzyka, o szczególnym znaczeniu dla firm funkcjonujących w ramach łańcuchów dostaw, jest ryzyko zakłóceń w przepływie informacji.

1. Przepływy w łańcuchu dostaw

W jednej z najpopularniejszych definicji łańcucha dostaw rozumianego jako „sieć powiązanych i współzależnych organizacji, które działając na zasadzie wzajemnej współpracy wspólnie kontrolują, kierują i usprawniają przepływy rzeczowe

[1] G. Montague-Jones, *Report exposes high cost of poor information flow in the supply chain*, 19-Nov-2010, www.foodproductiondaily.com (20.02.2011).

i informacji od dostawców do ostatecznych użytkowników”[2], wskazuje się na dwie grupy przepływów: przepływ dóbr i informacji. Kwestią bezsporną jest przynależność przepływów informacji do łańcucha dostaw. Informacja w łańcuchu dostaw podobnie jak w firmie traktowana jest jako zasób. Chopra i Meindl podkreślają, że informacja „służy jako łącznik między różnymi poziomami analizy łańcucha dostaw, umożliwiając koordynację wykonywanych działań i przynosząc w ten sposób wiele korzyści, przede wszystkim wzrost jego zyskowności”[3]. W literaturze przedmiotu podkreśla się strategiczne znaczenie przepływu informacji dla łańcucha dostaw, wskazując na podnoszenie jego zyskowności i możliwości osiągania przewagi konkurencyjnej. Najwięcej uwagi poświęca się kwestii dzielenia się informacją między poszczególnymi uczestnikami łańcucha dostaw, co umożliwia jego integrację i koordynację, może również przyspieszyć przepływ informacji, podnieść wydajność i efektywność łańcucha dostaw i umożliwić szybszą odpowiedź na zmiany w oczekiwaniach klientów.

Wyniki badań dotyczące wpływu dzielenia się informacją na proces realizacji zamówień wskazują, że prowadzi ono do większej przejrzystości łańcucha dostaw, a to umożliwia utrzymywanie niższych poziomów zapasów. Dzielenie się informacją w łańcuchu dostaw może obniżyć jego koszty o 12 do 23%[4]. G.P. Cachon i M. Fisher porównali tradycyjne sposoby wymiany informacji z wymianą informacji w relacjach partnerskich w łańcuchu dostaw i doszli do wniosku, że koszty związane z wymianą informacji mogą spaść do 2,2%[5]. Integracja między podmiotami wymieniającymi się informacjami w łańcuchu dostaw może doprowadzić do skrócenia czasów przepływu[6]. W bardzo wielu publikacjach wskazuje się również na możliwość zredukowania efektu „byczego bicza”. To właśnie brak przepływu albo przepływ nierzeczywistych informacji między ogniwami łańcucha dostaw prowadzi do efektu opisanego już w 1961 roku przez Forestera jako „akceleracja popytu”, a szerzej rozpowszechnionego przez Lee pod koniec lat 90. jako efekt „byczego bicza”[7]. Podaje się wiele powodów akceleracji popytu: fluktuacje cen, prognozowanie popytu „z nadwyżką”, zamawianie „na zapas” w celu zabezpiecze-

---

[2] M. Christopher, *Logistyka i zarządzanie łańcuchem dostaw*, Polskie Centrum Doradztwa Logistycznego, Warszawa 2000, s. 17.

[3] S. Chopra, P. Meindl, *Supply Chain Management. Strategy, Planning and Operation*, Pearson, New Jersey 2010, s. 23.

[4] H.L. Lee, K.C. So, C.S. Tang, *The value of information sharing in a two-level supply chain*, „Management Science” 2000, Vol. 46, No. 5, s. 626–643.

[5] G.P. Cachon, M. Fisher, *Supply chain inventory management and the value of shared information*, „Management Science” 2000, Vol. 46, No. 8, s. 1032–1048.

[6] R. Mason-Jones, D.R. Towill, *Total cycle time compression and the agile supply chain*, „International Journal of Production Economics” 1999, Vol. 62, No. 1–2, s. 61–73.

[7] H.L. Lee, V. Padmanabhan, S. Whang, *Information distortion in a supply chain: the Bullwhip effect*, „Management Science” 1997, Vol. 43, No. 4, s. 546-558.

nia się przed brakiem produktu. Jednak wszystkie wymienione działania mają swoje źródło w braku dostępu do rzetelnej informacji.

2. Ryzyko w łańcuchu dostaw

W literaturze dotyczącej ryzyka najczęściej przytacza się kategorie ryzyka proponowane przez T.T. Kaczmarka[8], Tarczyńskiego[9] czy Kulpę[10]: Wykorzystywane kategoryzacje ryzyka w praktyce gospodarczej odnoszą się do podziałów proponowanych w standardach zarządzania ryzykiem, przyjętych jednocześnie jako „najlepsze praktyki". Jednym z nich jest standard COSO. Zwykle wyróżnia się w nim cztery podstawowe obszary (poziomy) – ryzyka: strategiczne, operacyjne, finansowe oraz „inne". Obejmują one odpowiednio[11]:

- Ryzyko strategiczne dotyczące: wizerunku firmy – np. negatywny PR, osłabienie marki itp., niedostatku klientów, konkurencji, niekorzystnych trendów demograficznych i socjalnych, innowacji technologicznych, dostępności kapitału, sytuacji politycznej i regulacji prawnych, podatkowych itp.
- Ryzyko operacyjne związane z: funkcjonowaniem przedsiębiorstwa (np. rozwojem produktu, zasobami ludzkimi, wydajnością, wadami produktu i serwisu, zarządzaniem, cyklicznością w biznesie itp.), ograniczeniami wynikającymi ze słabego przywództwa, niezdolnością do zmian itp., sferą ICT, systemami sprawozdawczo-księgowymi (budżetowanie, planowanie, informacja księgowa, przygotowanie inwestycji itp.).
- Ryzyko finansowe dotyczące: cen (zmiany w kontekście kosztów oraz sytuacji na rynku), płynności finansowej (*cash flow*, zwł. spływ należności), kredytów (trudności ze spłatą, utrata zdolności kredytowej), inflacji/siły nabywczej, innych aspektów polityki finansowej.
- Ryzyko związane z niebezpieczeństwami, takimi jak: pożary i inne szkody majątkowe, klęski żywiołowe, kradzieże i inne przestępstwa, wypadki przy pracy, choroby, przerwy i zakłócenia w działalności firmy, odszkodowania.

Alternatywą dla przedstawionego sposobu klasyfikacji kategorii ryzyka, z jakimi mamy do czynienia w przedsiębiorstwie, może być podejście logistyczne, nawiązujące do usytuowania przedsiębiorstwa jako ogniwa w łańcuchu dostaw.

---

[8] T.T. Kaczmarek, *Zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Wyd. Difin, Warszawa 2010.

[9] W. Tarczyński, M. Mojsiewicz, *Zarządzanie ryzykiem. Podstawowe zagadnienia*, PWE, Warszawa 2001, s. 15.

[10] J. Brauer, *Rola i znaczenie zarządzania ryzykiem w logistyce globalnej*, INTLOG 2005, s. 3.

[11] W. Machowiak, *Zarządzanie ryzykiem w łańcuchu dostaw*, w: *Instrumenty zarządzania logistycznego*, red. M. Ciesielski, PWE, Warszawa 2008, s. 83.

Rozróżnia się w nim czynniki ryzyka zewnętrzne, na ogół całkowicie lub w dużym stopniu niezależne od decyzji podejmowanych w ramach zarządzania firmą, oraz wewnętrzne, będące pochodną realizowanych w nim procesów i podejmowanych decyzji.

Wśród zagrożeń zewnętrznych najczęściej wyróżnia się ryzyko występujące po stronie dostaw, po stronie sprzedaży (popytu) oraz „środowiskowe", związane z otoczeniem firmy i warunkami, w jakich działa.

Ryzyko po stronie dostaw to np. potencjalne zakłócenia dostaw materiałów i surowców, a także usług (w tym zwłaszcza w zakresie transportu), ich nieodpowiednia jakość, zmiany cen i warunków dostaw, wewnętrzne problemy dostawców itp. Z punktu widzenia lidera w łańcuchu dostaw (np. produkującego podstawowy asortyment) jest to ryzyko niezwykle groźne, gdyż prowadzi do przerw w produkcji bądź też nieadekwatnego do przyjętych i potencjalnych zamówień (zarówno w aspekcie ilościowym, jak i jakościowym) wywiązywania się przedsiębiorstwa z roli dostawcy, co może istotnie zagrozić wynikom firmy oraz jej wizerunkowi i pozycji na rynku.

Ryzyko występujące po stronie popytu to przede wszystkim konsekwencje zmiennej sytuacji na rynku, a więc: zmienność popytu, „wojny" cenowe, zachowania nie fair wobec konkurencji, a także kwestie relacji z odbiorcami (tu m.in. problemy ze spływem należności, problemy marketingowe, serwisowe i cały szereg innych).

Charakterystyczne dla strategii zarządzania łańcuchami dostaw jest pojawienie się całkowicie nowych, specyficznych dla tego poziomu integracji zagrożeń, które nie występują na poziomie przedsiębiorstwa. Należą do nich: konsekwencje braku jednego właściciela (bardzo istotne z punktu widzenia efektywności procesów decyzyjnych), ryzyko zakłóceń i zniekształceń w przepływie informacji, trudności z koordynacją działań czy ryzyko nielojalności partnerów (funkcjonujących przecież na ogół w różnych, często konkurujących łańcuchach dostaw) itp.

W przypadku wdrażania zarządzania ryzykiem na poziomie łańcucha dostaw kategoryzacja ryzyk i metodyka prac powinny być na tyle uzgadniane pomiędzy jego poszczególnymi ogniwami, aby umożliwić jednoznaczną komunikację, sprawny przepływ informacji, a przede wszystkim skuteczną koordynację działań.

3. Ryzyko zakłóceń w łańcuchu dostaw (zakłócona informacja)

Podczas wymiany informacji może dochodzić do jej zakłóceń w wyniku oddziaływania szumów, np. z otoczenia. Wśród podstawowych błędów w komunikacji wymienić należy: subiektywność odbiorcy w formułowaniu wniosków, zniekształcenie sensu przekazu na skutek zakłóceń, przerwanie komunikacji, dezorientację odbiorcy w wyniku wielowymiarowości komunikatu, powstanie konfliktu

dostawca–odbiorca na skutek różnic w percepcji i interpretacji przekazów, a także niezrozumienie w wyniku posługiwania się odmiennymi kodami znaczeniowymi[12].

Ryzyko zakłóceń w łańcuchu dostaw wynikać może między innymi z: naturalnych katastrof, bankructwa dostawcy, strajków pracowniczych, wojen, terroryzmu, niestabilności socjalno-ekonomiczno-politycznej.

Zakłócona informacja może być: mało przejrzysta, niewłaściwa, niepełna, niedokładna, nieweryfikowalna, pozbawiona integralności, poufności lub niedostępna.

Ryzyko zakłóceń charakteryzuje się niskim stopniem prawdopodobieństwa wystąpienia i dużą potencjalną stratą, podobnie jak zdarzenia katastrofalne, które mogą znacząco zakłócić lub opóźnić przepływy dóbr, informacji bądź finansów, co może zwiększyć koszty lub zrujnować przychody albo spowodować jedno i drugie naraz. Zarządzający łańcuchem dostaw mogą wybrać dwa komplementarne działania – chronić swój łańcuch dostaw lub rozwijać odporność łańcucha. Obecnie w literaturze nie ma wielu publikacji na temat zakłóceń w przepływie informacji w łańcuchu dostaw. Te, które się pojawiają, dotyczą pojedynczych zdarzeń, nie rozważa się jednak zależności między różnymi typami zakłóceń.

Innymi typami ryzyka związanymi również z niezakłóconym przepływem informacji są: ryzyko systemów i ryzyko własności intelektualnej.

Znaczenie ryzyka własności intelektualnej wzrosło wraz z wertykalną integracją łańcuchów dostaw i ich globalizacją oraz z chwilą, kiedy to firmy zaczęły zaopatrywać się – często poprzez outsourcing – u tych samych dostawców co ich konkurenci. Zyskowność firm zależy w dużej mierze od utrzymania przewagi konkurencyjnej, a w sytuacji swoistego rozlewu informacji na wszystkie podmioty w sieci dostaw utrzymanie takiej przewagi wynikającej np. z *know-how* staje się coraz trudniejsze.

Z kolei ryzyko systemowe jest jakby wtórne wobec ryzyka zakłóceń w przepływie informacji. Przedsiębiorstwa chcąc przyspieszyć, upewnić przepływy informacji, coraz częściej posługują się systemami informatycznymi. Jednak w wyniku ich stosowania rodzą się kolejne zagrożenia. Im większa sieć, w której działa przedsiębiorstwo, tym większe prawdopodobieństwo, że zagrożenie, które pojawi się gdziekolwiek, dotknie wszystkich uczestników sieci. Czyli skala ryzyka zakłóceń rozszerza się. Chociaż rzadkie, to zakłócenia bądź przerwy w przepływie informacji mogą jednak zniszczyć całą sieć powiązanych przedsiębiorstw. Przykładowo wirus Love Bug w 2002 roku spowodował zamknięcie poczty elektronicznej w Pentagonie, NASA i Fordzie, a dla wielu innych firm miliardowe straty. Dlatego obecnie przedsiębiorstwa duplikują wszystkie dane i transakcje, aby w wypadku zakłócenia system natychmiast wrócił do stanu początkowego. Niemniej istotne jest tutaj pra-

[12] G. Wieteska, *Zarządzanie ryzykiem w łańcuchu dostaw na rynku B2B*, Wyd. Difin, Warszawa 2011, s. 71.

widłowe wdrożenie procedur zarządzania ryzykiem. Znane są przypadki kiedy to w firmie duplikuje się dane, ale utrzymuje je na serwerach fizycznie zlokalizowanych w tym samym pomieszczeniu, w którym funkcjonuje zasadniczy system – w przypadku chociażby pożaru jeden i drugi ulegnie zniszczeniu.

Efektywne dzielenie się informacją w łańcuchu dostaw umożliwia oczywiście Internet i e-business, jednak zaadaptowanie przepływu informacji za pośrednictwem Internetu nie zawsze przynosi korzyści, pisze o tym Wagner we wnioskach dotyczących badań przeprowadzonych wśród małych i średnich przedsiębiorstw w Szkocji[13]. Tak więc dopiero koordynacja działań między firmami, a nie samo dzielenie się informacją, prowadzi do lepszych osiągnięć[14].

Wraz z rozwojem innowacji technologicznych zwiększa się ryzyko uzależnienia od nich procesów przepływu w łańcuchu dostaw. W związku z zastosowaniem nowych rozwiązań, zwłaszcza z zakresu technologii informatycznych, pojawiają nieznane dotąd zagrożenia. Niepożądanymi zdarzeniami informacyjnymi o charakterze technicznym są: awarie systemów, przerwy w dostawie mediów, brak możliwości dostępu do haseł, kluczy, akceptacji (z powodu np. choroby uprawnionego pracownika), bankructwo producenta komputerów, złośliwość przedmiotów martwych (prawa Murphy'ego), infekcja, atak wirusem komputerowym (robaki, konie trojańskie, bomby wirusowe, zapadnie, *spoofing* i inne), a także działania przypadkowych włamywaczy systemowych. Do jednych z najgroźniejszych realnych zamachów na zasoby informacyjne można zaliczyć tzw. ataki socjotechniczne[15]. Należy więc pamiętać, że Internet może stanowić również potencjalne źródło zagrożeń dla firm[16].

Informacja podczas przekazywania i przechowywania narażona jest na wiele zakłóceń. Rozwój infrastruktury informacyjnej i komunikacyjnej jest źródłem problematyki związanej ze standaryzacją, bezpieczeństwem, dostępnością i efektywnym jej wykorzystaniem. Bardzo ważnym zagadnieniem jest bezpieczeństwo informacji i bezpieczeństwo informatyczne. Zwiększanie poziomu bezpieczeństwa informacji w przedsiębiorstwie może obejmować następując obszary i działania. Komputery chronione są hasłem dostępu znanym tylko jego użytkownikom, dostęp do systemów i usług informacyjnych opiera się na procedurze rejestrowania i wyrejestrowania, wejście osób nieuprawnionych na teren organizacji jest ściśle nadzorowane, podpisywane są umowy o zachowaniu poufności (z pracownikami, firma-

---

[13] B.A. Wagner, I. Fillis, U. Johansson, *E-business and e-supply strategy in small and medium sized businesses* (SMEs), „Supply Chain Management: An International Journal" 2003, 8 (4), s. 343–354.

[14] S.M. Disney, M.M. Naim, A. Potter, *Assessing the impact of e-business on supply chain dynamics*, International Journal of Production Economics" 2004, s. 109–118.

[15] K. Młynarczyk, *Najsłabszy element – człowiek*, „Elektroniczna Administracja", marzec–kwiecień 2006, s. 57–63.

[16] G. Wieteska, *op. cit.*, s. 95.

mi), prowadzony jest nadzór informacji przychodzącej i wychodzącej firmy oraz nad dokumentami i zapisami, pracownicy są regularnie szkoleni w celu wzrostu ich świadomości w zakresie bezpieczeństwa informacji oraz redukcji prawdopodobieństwa błędów przez nich popełnianych. Firmy powinny również odpowiednio chronić bazy informacji, stosując skuteczne zabezpieczenia oraz systemy detekcji incydentów. Ponadto ważna jest też ochrona sprzętu informatycznego przed zagrożeniem typu: pożar, awaria zasilania, a także okablowania służącego do przesyłania danych przed potencjalnym przejęciem lub uszkodzeniem.

Podsumowanie

Przepływ informacji jest jednym z dwóch głównych typów przepływów wyróżnianych w łańcuchach dostaw. W strategiach łańcuchów dostaw kładzie się coraz większy nacisk na przepływ informacji i wykorzystanie narzędzi informatycznych. Generuje to jednak szereg nowych zagrożeń dla funkcjonowania w sieci, na skalę globalną. Należy więc uwzględniać informację jako kluczowy element dotyczący zarządzania ryzykiem w łańcuchu dostaw, gdyż informacja ta musi być odpowiednio zabezpieczona przed zakłóceniami.

Literatura

1. Brauer J., *Rola i znaczenie zarządzana ryzykiem w logistyce globalnej*, INTLOG 2005.
2. Cachon G.P., Fisher M., *Supply chain inventory management and the value of shared information*, „Management Science" 2000, Vol. 46, No. 8.
3. Chopra S., Meindl P., *Supply Chain Management. Strategy, Planning, and Operation*, Pearson, New Jersey 2010.
4. Christopher M., *Logistyka i zarządzanie łańcuchem dostaw*, Polskie Centrum Doradztwa Logistycznego, Warszawa 2000.
5. Disney S.M., Naim M.M., Potter A., *Assessing the impact of e-business on supply chain dynamics*, „International Journal of Production Economics" 2004, 89.
6. Kaczmarek T.T., *Zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Wyd. Difin, Warszawa 2010.
7. Lee H.L., So K.C., Tang C.S., *The value of information sharing in a two-level supply chain*, „Management Science" 2000, Vol. 46, No. 5.
8. Lee H.L., Padmanabhan V., Whang S., *Information distortion in a supply chain: the Bullwhip effect*, „Management Science" 1997, Vol. 43 No. 4.
9. Machowiak W., *Zarządzanie ryzykiem w łańcuchu dostaw*, w: *Instrumenty zarządzania logistycznego*, red. M. Ciesielski, PWE, Warszawa 2008.

10. Mason-Jones R., Towill D.R., *Total cycle time compression and the agile supply chain*, „International Journal of Production Economics" 1999, Vol. 62, No. 1–2.
11. Młynarczyk K., *Najsłabszy element – człowiek,* „Elektroniczna Administracja", marzec–kwiecień 2006.
12. Montague-Jones G., *Report exposes high cost of poor information flow in the supply chain*, 19-Nov-2010, www.foodproductiondaily.com (20.02.2011).
13. Tarczyński W., Mojsiewicz M., *Zarządzanie ryzykiem. Podstawowe zagadnienia*, PWE, Warszawa 2001.
14. Wagner B.A., Fillis I., Johansson U., *E-business and e-supply strategy in small and medium sized businesses (SMEs)*, „Supply Chain Management: An International Journal" 2003, 8 (4).
15. Wieteska G., *Zarządzanie ryzykiem w łańcuchu dostaw na rynku B2B*, Wyd. Difin, Warszawa 2011.

DISRUPTION RISK OF THE INFORMATION FLOW IN THE SUPPLY CHAIN

Summary

The information flow is one of two main types of distinguished flows in supply chains. The strategies of supply chains is placed increasing emphasis on information flow and use of IT tools. However, this generates a number of new threats to the functioning of the network on a global scale. It is, therefore, include the information as a key element for risk management in the supply chain, since this information must be adequately protected against disruptions.

Translated by Sylwia Konecka