ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 718 FINANSE. RYNKI FINANSOWE. UBEZPIECZENIA NR 53 2012

BOŻENA NADOLNA
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

WPŁYW ELEKTRONICZNEJ WYMIANY DANYCH (EDI) NA FUNKCJONOWANIE KONTROLI ZARZĄDCZEJ W JEDNOSTKACH SEKTORA FINANSÓW PUBLICZNYCH

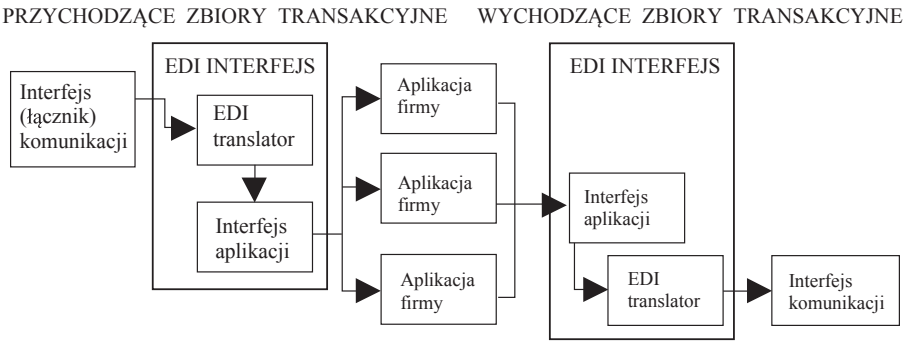
Wprowadzenie

Zadania realizowane przez jednostki sektora finansów publicznych powodują ciągły wzrost ilości dokumentów, co wiąże się z problemami związanymi z koordynacją działań podczas ich gromadzenia, spadkiem szybkości ich przetwarzania i przesyłania. Remedium na zwiększenie efektywności pozyskiwania i przetwarzania informacji może być wprowadzenie elektronicznej wymiany danych (ang. *EDI – Electronic Data Interchange*). Wdrożenie wymiany informacji w formie elektronicznej w jednostkach sektora finansów publicznych oddziałuje na narzędzia i procedury oceny realizacji zadań dokonywane w ramach kontroli zarządczej. Stosowanie narzędzi informatycznych ma bowiem wpływ na wszystkie elementy kontroli zarządczej, a w szczególności na środowisko wewnętrzne oraz informację i komunikację.

Celem artykułu jest przedstawienie istoty elektronicznej wymiany danych (EDI) oraz jej wpływu na funkcjonowanie kontroli zarządczej w jednostkach sektora finansów publicznych.

1. Istota elektronicznej wymiany danych (EDI)

Elektroniczna wymiana danych (ang. *EDI – Electronic Data Interchange*) jest formą wymiany informacji między komputerowymi systemami różnych organizacji. Oznacza ona bezpośrednią wymianę zestandaryzowanych dokumentów i komunikatów przekazywanych drogą elektroniczną[1] między komputerami dwóch organizacji[2]. Określa się ją również jako „sposób komunikowania się organizacji biorących udział w przedsięwzięciu gospodarczym, administracyjnym lub innym, polegającym na automatycznym przesyłaniu elektronicznie sformatowanych dokumentów[3]. Wymiana ta odbywa się w sposób automatyczny bez udziału człowieka. Istotę funkcjonowania EDI przedstawia rysunek 1.



Rysunek 1. Architektura systemu EDI

Źródło: J.V. Hansen, N.C. Hill: *Control and Audit of Electronic Data Interchange*, MIS Quarterly/December, 1989, s. 408.

Przedstawione na rysunku 1 rozwiązanie zakłada integrację wewnętrznego oprogramowania firmy z systemem wymiany EDI na poziomie wymiany plików. Interfejs komunikacji przekazuje dokument do translatora EDI, który przekłada format EDI dokumentu na format firmowych aplikacji informatycznych. Interfejs aplikacji z kolei akceptuje wejście dokumentu z translatora EDI i udostępnia

[1] Przekazywanie danych za pomocą sprzętu elektronicznego do przetwarzania danych (włącznie z kompresją cyfrową) z wykorzystaniem przekazu kablowego, radiowego, technologii optycznych lub jakiegokolwiek innego środka elektromagnetycznego.

[2] K. Anderson: *EDI and Data Network in the Public Sector*, Springer, 1998, s. 2.

[3] S. Kot, M. Starosta-Patyk, D. Krzywda: *Zarządzanie łańcuchem dostaw*, WWZPCz, Częstochowa 2009, s. 61.

mu właściwą aplikację firmy, na przykład pochodzącą z systemu ERP. Po sprawdzeniu kompletności i zgodności formatu danych w dokumencie zasila się nimi odpowiedni system informatyczny firmy. W przypadku wychodzących dokumentów proces ten przebiega odwrotnie.

Wynika z powyższego, że podstawową funkcją EDI jest transfer danych między wymieniającymi się partnerami, instytucjami czy osobami w warunkach uzyskania zgodności własnego formatu danych z formatem wymaganym przez protokół transmisji danych. Protokół ten jest opracowany na bazie określonego standardu. Standardy te są niezbędne, aby używać tego samego języka komunikacji przez osoby wymieniające między sobą informacje za pomocą EDI. Standardy EDI mogą być opracowywane dla poszczególnych dziedzin przez różne organizacje. Organizacje te są odpowiedzialne za definiowanie szablonów wiadomości, ich składni oraz zasad komunikacji[4]. Podstawą ich opracowywania są zazwyczaj dwa ogólne standardy: amerykański standard – ANSIX.12 oraz standard najczęściej stosowany w Europie opracowywany i rozwijany pod auspicjami ONZ – EDIFACT (ang. *Electronic Data Interchange for Administration, Commerce and Transport*)[5]. Standardy te umożliwiają tłumaczenie dokumentów wewnętrznych na język zrozumiały dla jego odbiorcy. Odbiorca może pobierać stosowne dane z dokumentu, uzupełniać nimi swoją dokumentację, archiwizować uzupełniony dokument lub przesyłać go dalszym użytkownikom występującym w łańcuchu EDI. Zakres zastosowań tych standardów jest szeroki. Przykładowo w ramach standardu ANSI.12 zostały opracowane następujące standardy dziedzinowe[6]:

— ASCX12A – edukacja i administracja,
— ASCX12C – komunikacja i kontrola,
— ASCX12F – finanse,
— ASCX12G – komunikacja rządowa,
— ASCX12H – gospodarka materiałowa,

[4] Standardy komunikacji określają rodzaj danych przekazywanych od nadawcy do odbiorcy, standardy składni natomiast definiują ogólny format dokumentu. Z kolei standardy komunikacji określają nazwę wiadomości oraz miejsce określonej informacji we wiadomości. Przy czym komunikaty mogą być przesyłane za pomocą dowolnego medium, jednakowego po obu stronach transmisji (http://infonomika.uek.kraków.pl).

[5] Celem stworzenia EDIFACT było uzyskanie uniwersalnego formatu dokumentu elektronicznego w skali międzynarodowej. Stanowi on swoisty rodzaj kompromisu między komunikatywnością przesyłanych danych a potrzebami w zakresie pozyskiwania danych w różnych dziedzinach gospodarki.

[6] R. Wojtachnik: *Elektroniczna wymiana dokumentów*, Mikom, Warszawa 2004, s. 56.

— ASCX12I – transport,
— ASCX12J – technika,
— ASCX12M – dystrybucja,
— ASCX12N – ubezpieczenia.

Również w ramach standardu EDIFACT są tworzone standardy ukierunkowane na potrzeby danej branży, jak na przykład: EANCOM opracowany dla handlu detalicznego i hurtowego uwzględniający strukturę kodu kreskowego.

Ponadto standard EDIFACT uwzględnia podobnie jak ANSI12 dokumenty takich branż, jak: przemysł, transport, finanse, ubezpieczenia czy sektor publiczny.

Dokumenty w standardzie EDIFACT są dzielone na trzy grupy:
— dokumenty handlowe umożliwiające wymianę informacji między stronami biorącymi udział w transakcji, należą do nich na przykład faktury elektroniczne, katalogi cenowe itd.
— dokumenty transportowe niezbędne do organizacji dostaw, na przykład awizo lub zlecenie transportowe,
— dokumenty finansowe związane z realizacją płatności (przelewy) i pozyskanie informacji o zmianach na kontach bankowych.

W procesie wymiany dokumentów elektronicznych można korzystać również ze standardu, który jest zintegrowany z technologiami internetowymi – XML (ang. *Exensible Markup Language*)[7]. Jest on niezależny od platformy sprzętowej i systemu operacyjnego, co oznacza, że nie istnieje tutaj konieczność instalacji sieci prywatnych i korzystania z usług pośrednika świadczącego usługi przesyłania danych.

Proces wymiany informacji w EDI odbywa się za pomocą sieci komunikacyjnych. Obecnie najczęściej stosowane są:
— połączenia dwupunktowe realizowane za pomocą mobilnych lub stacjonarnych modemów lub kart sieciowych przystosowanych do określonej infrastruktury teleinformatycznej,
— połączenia przy wykorzystaniu technologii sieci usług dodanych (ang. *VAN – Value Added Network*).

W pierwszym przypadku komunikacja między systemami informatycznymi poszczególnych jednostek jest realizowana bez pośrednika. Aplikacje partnerów biznesowych komunikują się bezpośrednio, przez serwery FTP, najczęściej za

[7] XML często jest określany jako rozszerzalny język programowania. Stanowi on zespół reguł pozwalających użytkownikowi tworzyć własne języki opisu określonych klas dokumentów.

pomocą połączeń internetowych, w których wprowadzono dodatkowe zabezpieczenia transmisji danych.

W technologii usług dodanych z kolei korzysta się z usług pośrednika-operatora, który centralnie zarządza danymi (dokumentami). Jednostka przesyła dokumenty elektroniczne do operatora, a ten przekazuje je do ich odbiorcy. W tej sytuacji VAN funkcjonuje jako biuro rozliczeń dla transakcji realizowanych za pomocą elektronicznych usług pocztowych o dużej szybkości przesyłania danych. Operatorami są wyspecjalizowane firmy informatyczne. W Polsce na przykład są to spółki: Comarch, Edison, Infinitie czy Xtrade.

Korzystanie z Sieci Wartości Dodanej (VAN) przy wymianie dokumentów elektronicznych posiada wiele zalet. Do podstawowych z nich zalicza się[8]:

— możliwość korzystania z dużej ilości różnych protokołów komunikacyjnych, co zwiększa elastyczność przesyłania danych w dokumentach,
— zwiększenie bezpieczeństwa przesyłania dokumentów od skrzynki pocztowej nadawcy do odbiorcy, za którą odpowiada operator,
— obniżenie kosztów związanych z zabezpieczeniami przesyłania danych oraz konserwacją wysoko specjalistycznego sprzętu, który jest własnością operatora; jednostka płaci tylko za abonament,
— możliwości skorzystania z dodatkowych usług typu: katalogi elektroniczne, wszelkiego rodzaju bazy danych, usługi płacenia elektronicznego, poczta elektroniczna itd.

W świetle powyższych rozważań wydaje się, że nie ma przeciwwskazań, aby jednostki sektora finansów publicznych w przypadku wdrażania EDI korzystały z usług operatora. Propozycje tego typu usług dla sektora publicznego w swej ofercie posiadają wszyscy polscy operatorzy EDI.

2. Przesłanki stosowania EDI w jednostkach sektora finansów publicznych

Do głównych przesłanek stosowania EDI w jednostkach sektora publicznego zalicza się:

— redukcję papierowych dokumentów i skrócenie czasu ich obiegu,
— wyższy poziom obsługi interesantów,

[8] EDISON. S.A. Podstawy EDI, http://www.edi.pl (5.06.2012).

— możliwość uniknięcia problemów związanych z tak zwanym „czynnikiem ludzkim", a więc zagubieniem dokumentów, błędnie wypisywanymi rozliczeniami na dokumentach,
— bieżącą dostępność do dokumentów elektronicznych bez konieczności przeszukiwania segregatorów oraz możliwość unikania innych problemów związanych z papierowym ich archiwizowaniem,
— obniżenie kosztów związanych ze zmniejszeniem zatrudnienia, zużyciem papieru, przesyłaniem i archiwizowaniem dokumentów,
— wprowadzenie regulacji prawnych umożliwiających stosowanie EDI w jednostkach sektora finansów publicznych.

Większość z wymienionych przesłanek dotyczy korzyści ze stosowania EDI, które zostały szeroko omówione w literaturze przedmiotu[9]. Największy wpływ na rozpowszechnienie EDI miały jednak regulacje prawne, które umożliwiły wprowadzenie EDI również w sektorze publicznym. Dotyczy to ustawy z dnia 18 września 2001 r. o podpisie elektronicznym[10] oraz ustawy z dnia 17 grudnia 2010 roku w sprawie przesyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej[11]. Zgodnie z zapisami tej ostatniej wystawianie i przesyłanie faktur w formie elektronicznej jest możliwe, jeżeli spełnione są łącznie dwa warunki:
— odbiorca faktur zaakceptował sposób przesyłania faktur w tej formie,
— została zapewniona autentyczność pochodzenia i integralność treści faktury.

Przy czym akceptacja odbiorcy może być wyrażona w formie pisemnej lub w formie elektronicznej.

Zapewnienie autentyczności pochodzenia i integralności treści faktury z kolei sprowadza się do[12]:

[9] B. Cox, S. Ghoneim: *Strategic use of EDI in the public sector: the HMSO case study*, Journal of Strategic Information Systems, 1998, (7) s. 39; K. Anderson, *EDI and Data Network in the Public Sector*, Springer, 1998, s. 134–137.

[10] Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. nr 130, poz. 1450 z późn. zm.). Zgodnie z zapisami tej ustawy podpis elektroniczny powinien być weryfikowany za pomocą ważnego, kwalifikowanego certyfikatu.

[11] Rozporządzenie Ministra Finansów z 17 grudnia 2010 r. w sprawie przesyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej (Dz.U. nr 249, poz. 1661).

[12] § 2 Rozporządzenia Ministra Finansów z 17 grudnia 2010 r. w sprawie przesyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej.

— autentyczności pochodzenia faktury, co oznacza pewność odnośnie do tożsamości dokonującego dostawy towarów lub usługodawcy albo wystawcy faktury,
— integralności treści faktury, przez co rozumie się, że w fakturze nie zmieniono zawartych w niej danych.

Z zapisów rozporządzenia wynika również, że autentyczność i integralność treści faktury są w szczególności zachowane w przypadku wykorzystania:
— bezpiecznego podpisu elektronicznego w rozumieniu art. 3 pkt 2 ustawy z 18 września 2001 r. o podpisie elektronicznym, weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu,
— elektronicznej wymiany danych (EDI), zgodnie z umową w sprawie europejskiego modelu wymiany danych elektronicznych, jeżeli zawarta umowa dotycząca tej wymiany przewiduje stosowanie procedur gwarantujących autentyczność pochodzenia faktury i integralność jej danych.

Sformułowanie „w szczególności" w treści tego zapisu wskazuje, że nie są to jednak wymogi konieczne, aby uznać fakturę za autentyczną.

Inną regulacją, która jest związana z wprowadzeniem EDI w sektorze publicznym, jest projekt ustawy z dnia 11 czerwca 2012 r. o zmianie ustawy o systemie ubezpieczeń oraz zmianie niektórych ustaw w związku z wdrożeniem Systemu Elektronicznej Wymiany Informacji dotyczących Zabezpieczenia Społecznego (EESSI) na terytorium Rzeczypospolitej Polskiej.

Konsekwencją tej ustawy ma być szybsze rozpatrywanie wniosków i należnych świadczeń na rzecz osób uprawnionych, pracujących i zamieszkałych na terenie Unii Europejskiej. Ustawodawca unijny założył, że wymiana danych między państwami członkowskimi odpowiedzialnymi za realizację przepisów europejskich w zakresie koordynacji zabezpieczenia społecznego odbywać się będzie drogą elektroniczną z wykorzystaniem wspólnej, bezpiecznej sieci – s-TESTA.

Kluczowym elementem architektury EESSI (ang. *Electronic Exchange of Social Security Information*) na poziomie krajowym będą tak zwane punkty kontaktowe, które w Polsce zostaną utworzone w Ministerstwie Pracy i Polityki Społecznej, w Zakładzie Ubezpieczeń Społecznych oraz w Narodowym Funduszu Zdrowia. Polskie instytucje zabezpieczenia społecznego powinny być przygotowane do korzystania z systemu EESSI najpóźniej do 1 maja 2014 r.

Omawiane przepisy wskazują również, że wdrażając EDI należy mieć świadomość występujących zagrożeń. Do podstawowych z nich należy bezpie-

czeństwo informacji w przesyłanych dokumentach[13]. Przeciwdziałać temu mają metody kryptograficzne, które są obecnie najczęściej używaną metodą uwierzytelniania i ochrony przed nieupoważnionym dostępem do danych.

Ponadto wdrożenie EDI w jednostkach sektora finansów publicznych najczęściej wiąże się ze zmianami w rozwiązaniach organizacyjnych, systemie rachunkowości oraz kontroli zarządczej.

3. Kontrola zarządcza w warunkach stosowania EDI

Kontrola zarządcza, stanowiąc ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy, wymaga uwzględnienia środowiska, w którym jest realizowana. Obecnie większość zadań w jednostkach sektora finansów publicznych jest wykonywana w środowisku informatycznym, obejmującym również EDI. Infrastruktura informatyczna w poszczególnych jednostkach jest różnorodna i podlega ciągłym zmianom. W związku z tym podstawową kwestią przy budowie modelu kontroli zarządczej w danej jednostce jest rozważenie zakresu oddziaływania tego środowiska na zadania realizowane przez jednostkę oraz działania kontrolne w ich zakresie. Sprawa jest tym bardziej istotna, iż zarządzający jednostką powinien mieć świadomość oddziaływania narzędzi informatycznych na wszystkie obszary kontroli zarządczej.

Do kontroli w warunkach stosowania technologii informacyjnej odnosi się przewodnik do standardów kontroli wewnętrznej dla sektora publicznego wydany przez INTOSAI. Zgodnie z jego zapisami korzystanie z technologii informacyjnej w jednostkach sektora finansów publicznych implikuje specyficzne typy działań kontrolnych obejmujące[14]:

— kontrolę ogólną,
— kontrolę aplikacji.

Kontrola ogólna dotyczy struktury, polityki i procedur, które mają zastosowanie do wszystkich lub większości jednostkowych systemów informatycznych i pomagają zabezpieczyć ich właściwe działanie. Tworzą one otoczenie,

[13] C. Hardy, R. Reeve: *A study of the internal control structure for electronic data interchange systems using the analytic hierarchy process*, „Accounting and Finance", 2000 (40), s. 192–194, K.V. Andersen, N.B. Andersen, N.C. Juul. EDIFACT in Denmark: *Proceedings of the 11th International Bled Electronic Commerce Conference*, 1998, Bled Slovenia, s. 126–132.

[14] *Guidelines for Internal Control Standards for the Public Sector*, INTOSAI GOV 9100, s. 32.

w którym systemy informatyczne działają i są kontrolowane. Dotyczy to również wdrażania EDI.

Kontrola aplikacji z kolei to badanie struktury, polityki i procedur, które mają zastosowanie do indywidualnych systemów informatycznych. Te kontrole są generalnie przeprowadzane w celu przeciwdziałania, wykrywania i korygowania błędów i nieprawidłowości w przepływach informacji w samych systemach informacyjnych danej organizacji i między nimi, jak i między systemami informacyjnymi innych organizacji. Zakres działań kontrolnych w obydwu obszarach przedstawia tabela 1.

Tabela 1

Działania w zakresie kontroli ogólnej i kontroli aplikacji
w warunkach stosowania technologii informacyjnych

Rodzaj kontroli	**Charakterystyka kontroli**
Kontrola ogólna	
Program ochrony danych i zarządzania nimi	Zakres i działania zarządzania ryzykiem, rozwój polityki ochrony danych, ocena odpowiedzialności, monitorowanie adekwatności kontroli w zakresie infrastruktury informatycznej.
Kontrola dostępu	Ograniczenia w zakresie kontroli dostępu do zasobów (danych, programów, wyposażenia i pomieszczeń), aby chronić te zasoby przed nieautoryzowanymi modyfikacjami, stratami i ujawnieniami. Kontrola dostępu obejmuje kontrolę fizyczną i logiczną.
Kontrola rozwoju, utrzymania i zmian w aplikacjach programowych	Zabezpieczenie przed nieautoryzowanymi programami lub modyfikacjami w istniejących programach.
Kontrola oprogramowania	Ograniczenia i monitorowanie dostępu do oprogramowania i zbiorów, które kontrolują oprzyrządowanie i zapewniają działanie aplikacji.
Podział obowiązków	Polityka, procedury i struktury organizacyjne są ustalone w taki sposób, aby zapobiec dokonywaniu kontroli przez jedną osobę we wszystkich kluczowych aspektach odnoszących się do operacji komputerowych.
Kontrola ciągłości usług	Pomoc w zapewnieniu, że w sytuacji nieoczekiwanych zdarzeń krytyczne operacje będą kontynuowane bez przerw lub będą niezwłocznie wznawiane, aby chronić kluczowe i poufne dane.

Rodzaj kontroli	Charakterystyka kontroli
Kontrola aplikacji	
Kontrola wejść do systemu	Dane są autoryzowane, przekształcone w sposób prawidłowy na formę elektroniczną, w aplikacjach informatycznych jednostki są dokładnie odzwierciedlone, kompletne i terminowe.
Kontrola przetwarzania	Dane są prawidłowo przetwarzane przez komputer i zbiory są poprawnie aktualizowane.
Kontrola wyjść z systemu	Zbiory i raporty generowane przez aplikację odpowiadają transakcjom lub zdarzeniom, które aktualnie są realizowane i dokładnie odzwierciedlają rezultaty przetwarzania, raporty są kontrolowane i dystrybuowane przez autoryzowanych użytkowników.

Źródło: *Guidelines for Internal Control Standards for the Public Sector*, INTOSAI GOV 9100, s. 33.

Zgodnie ze standardami kontroli zarządczej swym zakresem obejmuje ona:
— środowisko wewnętrzne,
— cele i zarządzanie ryzykiem,
— mechanizmy kontroli,
— informacje i komunikację,
— monitorowanie i ocenę.

W odniesieniu do środowiska wewnętrznego kierownik jednostki powinien zadbać, aby osoby wykorzystujące w swojej pracy narzędzia informatyczne posiadały odpowiednie kompetencje, umiejętności i doświadczenie. Powinien również umożliwić im rozwój zawodowy oraz wspierać i promować właściwe zachowania etyczne, co w sytuacjach zapewnienia bezpieczeństwa danych jest szczególnie istotne. Wdrożenie EDI często wiąże się ze zmianami w zakresie zadań, uprawnień i odpowiedzialności poszczególnych komórek organizacyjnych. W gestii kierownika jednostki oraz podległych mu menadżerów leży wyraźne wskazanie w formie pisemnej na uprawnienia poszczególnych osób do wystawiania dokumentów w formie elektronicznej oraz ich kontroli, jak również wyznaczenie osób odpowiedzialnych za ich treść, terminowość oraz integralność. Kierownik jednostki powinien również wyraźnie określić zakres uprawnień delegowanych poszczególnym osobom zarządzającym lub pracownikom odnośnie do potwierdzania i kontroli dokumentacji wysyłanej i odbieranej drogą elektroniczną oraz wskazać osoby odpowiedzialne za bezpieczeństwo danych, jeżeli zależy ono od rozwiązań informatycznych stosowanych w jednostce. Przekazanie określonych obowiązków innemu pracownikowi nie zmienia jednak

odpowiedzialności kierownika jednostki za prawidłowo funkcjonującą kontrolę zarządczą.

Identyfikacja ryzyka w odniesieniu do realizacji celów i zadań w warunkach stosowania narzędzi informatycznych, w tym EDI, stanowi istotny element kontroli zarządczej. W tym celu powinno wypracować się w jednostce jednoznaczną politykę w zakresie analizy ryzyka. Wymaga to wyznaczenia:

— celów organizacji dotyczących zarządzania ryzykiem przy stosowaniu technologii informatycznych,
— akceptowanego poziomu ryzyka w zakresie systemów informatycznych i EDI,
— zasad i metod oceny ryzyka,
— osób odpowiedzialnych za zarządzanie ryzykiem,
— mechanizmów eliminowania ryzyka.

Identyfikacja ryzyka w odniesieniu do technologii informacyjnej obejmuje następujące działania:

— identyfikowanie zasobów i procesów informatycznych[15],
— określanie podatności tych zasobów i procesów na zagrożenia,
— ocenę prawdopodobieństwa nieautoryzowanego wykorzystania zasobów,
— szacowanie ewentualnych strat z tytułu zagrożeń w zasobach i procesach informatycznych,
— wyznaczenie mechanizmów przeciwdziałania ewentualnym zagrożeniom.

Przykładową identyfikację ryzyka związanego z fizycznym zabezpieczeniem zasobów przetwarzanych w ramach EDI przedstawia tabela 2.

[15] Procesy informatyczne są rozumiane jako planowane, realizowane lub monitorowane działania związane z pozyskiwaniem, przetwarzaniem i udostępnianiem informacji z wykorzystaniem narzędzi informatycznych. Na etapie pozyskiwania i udostępniania informacji może być wykorzystywane EDI.

Tabela 2

Identyfikacja ryzyka związanego z fizycznym zabezpieczeniem zasobów informacyjnych przetwarzanych i przesyłanych w ramach EDI

Kategoria ryzyka	Opis ryzyka
Brak planów lub niewłaściwe ich przygotowanie w zakresie fizycznego zabezpieczenia sprzętu i oprogramowania	Brak planów ochrony fizycznej budynków przed kradzieżą, pożarem, zalaniem. Brak planów bezpośrednich zabezpieczeń sprzętu. Brak harmonogramu okresowych przeglądów sprawności sprzętu bezpośrednio zabezpieczających system lub budynki.
Brak procedur w zakresie fizycznego zabezpieczania systemów	Brak procedur wydawania i zdawania kluczy do pomieszczeń. Brak procedur na wypadek nietypowych zdarzeń związanych z serwerami. Brak procedur w zakresie ochrony nośników danych.
Brak lub wadliwe funkcjonowanie zabezpieczeń przed fizycznym dostępem do systemu	Brak zabezpieczeń przeciwpożarowych. Brak środków ochrony przed zalaniem. Brak środków ochrony związanej z zasilaniem elektrycznym. Nieprawidłowy dobór zabezpieczeń do budynków i pomieszczeń ze sprzętem.
Brak testowania sprawności sprzętu służącego fizycznym zabezpieczeniom systemu	Brak testów zasilania awaryjnego. Brak okresowego sprawdzania sprawności zamków, monitoringu.
Brak informacji dla pracowników w zakresie stosowania procedur zabezpieczających	Brak szkoleń w zakresie stosowanych zabezpieczeń. Brak sprecyzowania zadań dla poszczególnych pracowników w zakresie stosowanych zabezpieczeń.

Źródło: opracowanie własne.

W celu przeciwdziałania ryzyku kierownictwo jednostki powinno stworzyć odpowiednie mechanizmy kontroli, które stanowią odpowiedź na konkretne ryzyko. W odniesieniu do systemów informatycznych i EDI istotnym jest określenie mechanizmów służących zapewnieniu bezpieczeństwa systemów informatycznych. Podstawowe atrybuty bezpieczeństwa systemów informatycznych przedstawia tabela 3.

Tabela 3

Atrybuty bezpieczeństwa systemów informatycznych

Atrybut	Charakterystyka
Poufność	Informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom.
Autentyczność	Tożsamość podmiotu lub zasobu jest zgodna z deklaracją. Dotyczy to użytkowników, procesów, systemów lub nawet instytucji.
Dostępność	Możliwość korzystania z danych na każde żądanie, w założonym czasie wyłącznie przez upoważnionego użytkownika.
Integralność danych	Dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Integralność systemu	System realizuje swoje funkcje w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.
Jednoznaczność	Działania podmiotu (np. użytkownika) mogą być jednoznacznie przypisane tylko temu podmiotowi.
Niezawodność	Zachowania systemu są zgodne z zamierzeniami użytkownika.

Źródło: opracowanie na podstawie PN-I-13335-1. Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcie i modele bezpieczeństwa systemów informatycznych. Katalog Polskich Norm, Baza Zintegrowanego Systemu Informatycznego NORMA, www.pkn.pl.

W odniesieniu do EDI wprowadzono tak zwane usługi ochrony, które obejmują obok kontroli dostępu, sprawdzania poufności i integralności danych oraz konieczności uwierzytelniania tożsamości podmiotu lub źródła danych również tak zwane pojęcie „niezaprzeczalności", czyli sytuacji, w której nadawca lub odbiorca nie będą mogli wyprzeć się faktu wystąpienia sesji lub jej treści.

Kontrola zarządcza w ramach informacji i komunikacji powinna sprowadzać się do oceny efektywności mechanizmów przekazywania informacji w obrębie struktury organizacyjnej jednostki, jak i poza nią w odniesieniu do tych jednostek, które mają wpływ na osiąganie jej celów i realizację zadań. Stosowanie EDI może ten proces znacznie usprawnić. W związku z tym kierownictwo jednostki powinno promować w jednostce kulturę w zakresie wykorzystania sieci informatycznych podczas realizacji jej zadań, rozpoznawać standardy teleinformatyczne realizowane w otoczeniu jednostki, posiadać znajomość regulacji prawnych w tym zakresie.

System kontroli zarządczej w zakresie prawidłowego funkcjonowania EDI w jednostce powinien podlegać bieżącemu monitorowaniu i ocenie. Ocena ta powinna dotyczyć między innymi:

— celowości stosowania EDI,
— zakresu zadań realizowanych przy pomocy EDI,
— bezpieczeństwa zasobów informacyjnych podczas ich przesyłania za pomocą EDI,
— uprawnień poszczególnych osób do dysponowania zasobami informacyjnymi przetwarzanymi i przesyłanymi za pomocą EDI.

Ponadto kierownictwo jednostki i pracownicy na każdym stanowisku powinni przeprowadzać samoocenę w zakresie prawidłowego funkcjonowania EDI w jednostce. Ze względu na znaczenie informacji w zarządzaniu jednostkami sektora finansów publicznych oraz konieczność ich ochrony przed nieupoważnionym dostępem również przetwarzanie i przesyłanie informacji za pomocą EDI powinno być poddane ocenie przez audytora wewnętrznego.

Uwagi końcowe

Pomyślne wdrożenie elektronicznej wymiany danych (EDI) w jednostce sektora finansów publicznych wymaga dużego zaangażowania jej kierownictwa oraz odpowiedniej infrastruktury informatycznej. Stosowanie EDI wpływa bowiem znacząco na inne systemy informacyjne przedsiębiorstwa oraz na funkcjonowanie kontroli zarządczej we wszystkich jej obszarach, mimo że podstawowe cele tej kontroli nie ulegają zmianom. Przeobrażenia w zakresie procedur kontroli zarządczej powinny zmierzać w kierunku utrzymania, a nawet podnoszenia jej efektywności. Efektywna kontrola stosowanej w jednostce technologii informacyjnej powinna dostarczać zarządzającym uzasadnionego zapewnienia, że gromadzone, przetwarzane i przesyłane informacje spełniają zamierzone cele kontroli, a więc są kompletne, terminowe, nienarażone na nieuprawniony dostęp i błędy oraz integralne.

Ponadto kierownik jednostki sektora finansów publicznych powinien mieć świadomość, że rozwój narzędzi internetowych oraz handlu elektronicznego będzie w coraz większym stopniu wpływać na istotę i konieczność wprowadzania specyficznych działań kontrolnych w tych jednostkach.

Literatura

Anderson K.: *EDI and Data Network in the Public Sector*, Springer, Heidelberg 1998.

Andersen K.V., Andersen N.B., Juul N.C.: *EDIFACT in Denmark*, Proceedings of the 11th International Bled Electronic Commerce Conference, 1998, Bled Slovenia.

Cox B., Ghoneim S.: *Strategic use of EDI in the public sector: the HMSO case study*, „Journal of Strategic Information Systems", 1998, nr 7.

EDISON S.A. *Podstawy EDI*, http://www.edi.pl (5.06.2012).

Guidelines for Internal Control Standards for the Public Sector, INTOSAI GOV 9100.

Hansen J.V., Hill N.C.: *Control and Audit of Electronic Data Interchange*, „MIS Quarterly", December 1989.

Hardy C., Reeve R.: *A study of the internal control structure for electronic data interchange systems using the analytic hierarchy process*, „Accounting and Finance", 2000.

Katalog Polskich Norm, Baza Zintegrowanego Systemu Informatycznego NORMA, www.pkn.pl.

Kot S., Starosta-Patyk M., Krzywda D.: *Zarządzanie łańcuchem dostaw*, WWZPCz, Częstochowa 2009.

Rozporządzenie Ministra Finansów z 17 grudnia 2010 r. w sprawie przesyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej (Dz.U. nr 249, poz. 1661).

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. nr 130, poz. 1450 z późn. zm.)

Wojtachnik R.: *Elektroniczna wymiana dokumentów*, Mikom, Warszawa 2004.

dr Bożena Nadolna
Zachodniopomorski Uniwersytet Technologiczny
Katedra Rachunkowości
Szczecin, ul. Żołnierska 47
bozena.nadolna@zut.edu.pl

EFFECT OF ELECTRONIC DATA INTERCHANGE (EDI) ON MANAGEMENT CONTROL IN THE PUBLIC SECTOR ENTITIES

Summary

In the era of rapid development of computer science information management is an essential element of the work of the head of public sector entity. In this regard, it uses the latest information technologies, including EDI.

This article presents the essence of EDI and its impact on management control. The paper first discusses the nature, advantages and disadvantages of EDI. It then discusses the conditions for the use of EDI in the public sector and management control in its environment.

Translated by Bożena Nadolna