

Grażyna Michalczuk, Łukasz Siemieniuk¹

PROBLEMATYKA BEZPIECZEŃSTWA KOMPUTEROWYCH SYSTEMÓW FINANSOWO- -KSIĘGOWYCH

Streszczenie

Rozwój technik informacyjno-komunikacyjnych determinuje przedsiębiorstwa do wdrażania najnowszych technologii w każdym obszarze ich funkcjonowania. Takim szczególnym obszarem jest rachunkowość. Stanowi ona sformalizowany, całościowy i uporządkowany system zapisu zdarzeń gospodarczych, zachodzących w przedsiębiorstwie. Jakość tego systemu warunkuje racjonalność podejmowanych decyzji. Z tego powodu systemy informatyczne, wspomagające rachunkowość, powinny być tak skonstruowane, aby rozwiązania oraz procedury w nich zastosowane spełniały kryteria zasad rachunkowości, a równocześnie w jak najlepszy sposób pomagały spełniać wymagania prawne, stawiane księgom rachunkowym.

Celem artykułu jest przedstawienie problematyki funkcjonowania systemów finansowo-księgowych w przedsiębiorstwie w aspekcie ich bezpieczeństwa.

Słowa kluczowe: systemy finansowo-księgowe, bezpieczeństwo systemów komputerowych, *Ustawa o rachunkowości*

SECURITY OF FINANCIAL AND ACCOUNTING COMPUTER SYSTEMS

Summary

The development of ICT prompts companies to implement the latest technologies in every area of their operation. Among these specific fields is accounting. It is a formal, comprehensive and structured system of recording economic events taking place in an enterprise. The quality of this system is crucial for the rationality of decision-making. Therefore, IT systems designed for accounting purposes should be constructed in such a way that the solutions and procedures they use comply with the accounting standards, and at the same time help, in the best possible way, to meet the legal requirements for accounting books.

Key words: financial and accounting systems, security of computer systems, *the Accounting Act*

Wprowadzenie

W dobie rozwijającej się komputeryzacji i cyfryzacji coraz więcej przedsiębiorstw decyduje się zrezygnować z tradycyjnego prowadzenia ksiąg rachunkowych

¹ dr Grażyna Michalczuk – Wydział Ekonomii i Zarządzania, Uniwersytet w Białymstoku; mgr Łukasz Siemieniuk – Wydział Ekonomii i Zarządzania, Uniwersytet w Białymstoku

na rzecz komputerowych programów finansowo-księgowych. Determinowane jest to nie tylko znacznym usprawnieniem pracy wewnątrz jednostki w zakresie finansów i rachunkowości, ale też ułatwieniem jej komunikacji z innymi instytucjami. Pozwala również na prostszy i zdecydowanie szybszy dostęp do danych, ich sprawdzenie oraz analizę.

Komputeryzacja działań finansowo-księgowych może okazać się ułatwieniem, a nie utrudnieniem pracy, w tym celu jednak należy zastanowić się nad wyborem konkretnego systemu finansowo-księgowego. Głównym zadaniem w tym zakresie jest dokładna analiza oferty komputerowych programów finansowo-księgowych, dostępnych na rynku, pod względem najistotniejszych cech z punktu widzenia potrzeb przedsiębiorstwa. Jest to bardzo istotne, ponieważ „spełnienie kryteriów użytkowych, czyli zakresu dostępnych w programie funkcji, zależy od potrzeb jednostki, od tego, które obszary rachunkowości chce zautomatyzować i jakie środki na ten cel przeznaczyć”². Wśród najważniejszych cech, na jakie należy zwrócić uwagę przy wyborze odpowiedniego dla przedsiębiorstwa systemu finansowo-księgowego, znajdują się m.in. system zabezpieczeń oprogramowania, łatwość w obsłudze systemu, koszty jego zakupu i wdrożenia, a także opinia o producencie oprogramowania³. Wśród wymienionych cech coraz większe znaczenie ma szeroko rozumiane bezpieczeństwo systemów finansowo-księgowych.

Celem artykułu jest przedstawienie problematyki funkcjonowania systemów finansowo-księgowych w przedsiębiorstwie w aspekcie ich bezpieczeństwa.

1. Wybrane aspekty bezpieczeństwa systemów finansowo-księgowych

Postępujący rozwój technik informacyjno-komunikacyjnych wymusza na przedsiębiorstwach konieczność wdrażania najnowszych technologii niemal w każdym obszarze jego działalności. Dotyczy to również prowadzenia rachunkowości, która stanowi uniwersalny, elastyczny, podmiotowy system informacyjny, umożliwiającą tworzenie liczbowego obrazu powstawania, podziału i przepływu wartości oraz związanych z tym rozrachunków między podmiotami gospodarczymi⁴. Rachunkowość jest systemem ewidencyjnym, który gromadzi, przetwarza i przekazuje odbiorcom zewnętrznym informacje finansowe, zgodnie z obowiązującym prawem bilansowym.

Powszechnie rachunkowość uznawana jest za język biznesu, który umożliwia porozumiewanie się wszystkim uczestnikom życia gospodarczego. Odzwierciedleniem takiego podejścia jest zdefiniowanie przez *American Institute of Certified*

² T. Cebrowska, *Rachunkowość finansowa i podatkowa*, Wydawnictwo Naukowe PWN, Warszawa 2010, s. 197.

³ Ibidem, s. 204.

⁴ G. Michalczuk, *Zasoby niematerialne jako czynnik wartości przedsiębiorstwa. Luka informacyjna sprawozdawczości finansowej*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2013, s. 270-271.

Public Accountants rachunkowości jako działalności usługowej, której zasadniczą funkcją jest dostarczanie informacji kwantytatywnych, głównie finansowych o jednostkach gospodarczych⁵. Informacje te służą do podejmowania decyzji ekonomicznych oraz dokonywania racjonalnych wyborów pomiędzy alternatywnymi kierunkami działania.

Z tego powodu systemy informatyczne, mające na celu wspomaganie finansów i rachunkowości, powinny być tak skonstruowane, aby rozwiązania oraz procedury w nich zastosowane spełniały kryteria zasad rachunkowości i były zgodne z wymogami ustawy o rachunkowości, a jednocześnie w jak najlepszy sposób spełniały wymogi bezpieczeństwa. Jest to o tyle istotny problem, że wykorzystanie programów finansowo-księgowych niesie za sobą szereg zagrożeń. Największym, a zarazem rozpowszechnionym, zagrożeniem bezpieczeństwa są hakerzy, których celem jest często przedostanie się do jednego z komputerów w sieci, a następnie za jego pośrednictwem zdobycie danych znajdujących się na urządzeniach firmowych. Kolejnym zagrożeniem są błędy oprogramowania, a w szczególności problemy występujące w systemie operacyjnym, serwisach sieciowych oraz innych programach wykorzystujących połączenia sieciowe⁶. Ponadto zagrożenia stanowią również wirusy, które wraz z upływem czasu stają się coraz bardziej nieprzewidywalne. Ogromny problem istnieje również w ułatwionym dostępie do komputera, wynikającym z stosowania prostych haseł dostępu, które nie stanowią problemu w ich złamaniu.

Zabezpieczenia, których zadaniem jest ochrona przed dostępem do programów finansowo-księgowych firmy oraz danych przez osoby z zewnątrz, są to zabezpieczenia dostępu logicznego. Kontrole dostępu logicznego mają za zadanie⁷:

- zapobieganie przed dostępem użytkowników nieuprawnionych;
- umożliwienie dostępu jedynie uprawnionym użytkownikom;
- zawężenie uprawnień dostępu upoważnionym użytkownikom;
- kontrolowanie czynności uprawnionych użytkowników.

W celu odpowiedniej realizacji zabezpieczeń dostępu logicznego przedsiębiorstwa powinny wykorzystywać: zabezpieczenia programowo-sprzętowe, zabezpieczenia w systemie operacyjnym, zabezpieczenia aplikacyjne oraz zabezpieczenia sieciowe.

Do grupy zabezpieczeń programowo-sprzętowych należą operacje takie jak: szyfrowanie informacji, wykonywanie kopii bezpieczeństwa, korzystanie z zasilania awaryjnego, a także z zapór sieciowych. Za najbardziej skuteczny sposób jest uznawane szyfrowanie. W szyfrowaniu wykorzystuje się funkcje matematyczne oraz hasła szyfrowania. Szyfrowanie polega na przekształcaniu informacji jawnej w inną, np. w postaci tekstu zaszyfrowanego⁸. W przypadku zasilania awaryjnego

⁵ A. Belkaoui, *Accounting Theory*, HBJ Publishers, San Diego 1985, s. 4.

⁶ K. Rytelewska, T. Siemieniuk, *Problematyka zabezpieczenia informacji w zintegrowanych systemach informatycznych*, [w:] *Systemy informatyczne, a funkcjonowanie organizacji gospodarczych*, N. Siemieniuk, J. Sikorski (red.), Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2011, s. 75.

⁷ *Bezpieczeństwo informatyczne – zabezpieczenia dostępu logicznego*, „Rachunkowość” 2004, nr 6, http://rachunkowosc.com.pl/artukul/200406/7/Bezpieczenstwo_informatyczne_-_zabezpieczenia_dostepu_logicznego [dostęp: 10.05.2014].

⁸ K. Rytelewska, T. Siemieniuk, op. cit., s. 79.

ma ono na celu ochronę sprzętu komputerowego przed nagłym wyłączeniem, a jednocześnie przed utratą danych.

Zabezpieczenia w systemach finansowo- księgowych mają za zadanie niedopuszczenie do swobodnego dostępu do danych, a przede wszystkim ich modyfikacji, przeprowadzanej w inny sposób niż przewidziany został w oprogramowaniu systemu. „Najczęstszym rozwiązaniem w praktyce jest wyposażenie systemu w program umożliwiający kontrolę kompletności zbiorów głównych, weryfikację obliczeń, badanie zgodności sum kontrolnych oraz powiązań rachunkowych i logicznych między zbiorami”⁹. Praca tego programu polega na automatycznym wykrywaniu wszelkich niespójności danych znajdujących się w treściach zbiorów, oraz weryfikacji przetwarzania i ujawniania niedozwolonych modyfikacji zawartości zbiorów¹⁰. Zabezpieczenie tego rodzaju wyznacza, do jakich danych, a także do jakiego oprogramowania po uruchomieniu komputera, ma dostęp użytkownik.

Zabezpieczenia aplikacyjne wyznaczają granice pracy użytkownika z daną aplikacją, taką jak np. nazwa użytkownika, której wpisanie wymagane jest przed uruchomieniem aplikacji księgi głównej, i która jednocześnie pozwala danemu użytkownikowi na przeglądanie danych, ale bez możliwości wprowadzania jakichkolwiek zmian. Natomiast zabezpieczenia sieciowe mają na uwadze ochronę przed nieuprawnionym dostępem do sieci komputerowej w danej jednostce. Zadaniem systemu jest ograniczenie dostępu do danych poprzez udostępnianie użytkownikom jedynie funkcji mu potrzebnych, bez przedstawiania mu innych możliwości. Ponadto dostęp do funkcji chroniony jest hasłem przed dostępem nieupoważnionych osób.

2. Wymogi ustawowe odnośnie komputerowych systemów finansowo-księgowych

Prowadzenie rachunkowości uregulowane jest przepisami ustawy o rachunkowości, która m.in. definiuje wymagania stawiane systemom komputerowym, wykorzystywanym w rachunkowości. Według przepisów ustawy o rachunkowości prowadzenie ksiąg rachunkowych przy użyciu komputera wymaga: 1) opisu systemu informatycznego, zawierającego wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, wraz z opisem algorytmów i parametrów; 2) stworzenia programowych zasad ochrony danych, w tym w szczególności metod zabezpieczenia dostępu do danych i systemu ich przetwarzania; 3) określenia wersji oprogramowania i daty rozpoczęcia jego eksploatacji; 4) opisu systemu służącego ochronie danych i ich zbiorów, w tym dowodów księgowych, ksiąg rachunkowych i innych dokumentów stanowiących podstawę dokonanych w nich zapisów¹¹.

⁹ M. Okuń, *Ochrona danych księgowych oraz systemów informatycznych pod rządami Ustawy o rachunkowości*, [w:] *Technologie informacyjne w finansach i rachunkowość*, N. Siemieniuk, J. Sikorski (red.), Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2003, s. 203.

¹⁰ Ibidem.

¹¹ *Ustawa z dnia 29 września 1994 r. o rachunkowości*, Dz. U. 2013, poz. 613 z późn. zm., art. 10.

Ustawa określa również „ogólne warunki przechowywania i ochrony dokumentacji opisującej zasady rachunkowości oraz zbiorów danych księgowych tworzonych w systemach informatycznych rachunkowości”¹². Według jej wymogów w jednostkach prowadzących księgi rachunkowe przy użyciu komputera, ochrona danych powinna polegać na: 1) stosowaniu odpornych na zagrożenia nośników danych, przy wykorzystaniu środków ochrony zewnętrznej; 2) systematycznym tworzeniu rezerwowych kopii zbiorów danych zapisanych na informatycznych nośnikach danych, przy założeniu trwałości zapisu informacji systemu rachunkowości, przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych; 3) zapewnieniu ochrony programów komputerowych i danych systemu informatycznego rachunkowości, poprzez stosowanie odpowiednich rozwiązań programowych i organizacyjnych, chroniących przed nieupoważnionym dostępem lub zniszczeniem¹³.

Według wymogów ustawy, aby system księgowy mógł być użytkowany, powinien spełniać szereg wymagań. Są to przede wszystkim¹⁴:

- wiarygodność danych;
- systematyczność ich wprowadzania;
- bezbłądność i możliwość sprawdzenia wprowadzanych danych.

Gromadzenie danych, zgodnie z ustawą o rachunkowości, wymaga także okresowej ich archiwizacji. Celem takiego wymogu jest minimalizacja ryzyka wynikającego z możliwości utraty danych z powodu: awarii sprzętu, wspomnianego już wirusa komputerowego czy też kradzieży. Archiwizacja zapewnia ponadto ochronę w przypadku błędu użytkownika. Ustawa nie określa natomiast częstotliwości archiwizowania danych. Uwarunkowane jest to niewątpliwie ilością i częstotliwością wprowadzanych danych. Z tego powodu częściej dokonywana archiwizacja naraża na mniejsze ryzyko utraty większej ilości informacji i konieczność ponownego ich zapisu; dlatego też w większości przedsiębiorstw archiwizację przeprowadza się po skończonej pracy każdego dnia roboczego¹⁵.

Z punktu widzenia zapewnienia rzetelności i kompletności gromadzonych przez rachunkowość informacji, ważną kwestią pozostaje również ochrona danych oraz oprogramowania. Z tego względu tak ważny jest wielopoziomowy system bezpieczeństwa, na który powinny się składać takie środki ostrożności jak¹⁶:

- system zabezpieczeń mechanicznych, chroniących sprzęt komputerowy przed zniszczeniem;
- system zabezpieczeń systemu operacyjnego, ograniczający dostęp poszczególnych osób do najważniejszych funkcji;

¹² M. Okuń, op. cit., s. 202.

¹³ Ustawa z dnia 29 września 1994 r. o rachunkowości, op. cit., art. 71.

¹⁴ Ł. Siemieniuk, *System Symfonia jako przykład zintegrowanego systemu informatycznego w rachunkowości*, „Optimum. Studia Ekonomiczne” 2011, nr 1, s. 219.

¹⁵ A. Ostaszewicz, *Bezpieczeństwo informatyczne – zabezpieczenia dostępu logicznego*, „Rachunkowość” 2004, nr 6, s. 12.

¹⁶ *Bezpieczeństwo informatyczne...*, op. cit.

- program ciągłego szkolenia pracowników w zakresie bezpieczeństwa danych firmy;
- właściwy system pracy oraz podział obowiązków w odniesieniu do różnych opcji programów;
- utrzymywanie zabezpieczeń systemów komputerowych oraz ich nieustanna kontrola.

Stosowane w większości firm zabezpieczenia ujmowane są w procedurach systemowych i procedurach organizacyjnych. Te pierwsze zawarte są jako funkcje programu komputerowego, te drugie zaś zależą tylko i wyłącznie od użytkownika określonego komputerowego systemu finansowo-księgowego. Procedury organizacyjne mają na celu zapobieganie zniszczeniu danych i są niezależne od rodzaju oprogramowania komputerowego, jakie zostało wdrożone w danej firmie. Zaliczyć do nich można takie zabezpieczenia jak: ochrona sprzętu przed zdarzeniami losowymi, np. pożarem czy kradzieżą, a także mniej lub bardziej zaawansowane programy antywirusowe, uniemożliwiające zainfekowanie sprzętu, jak również całej sieci komputerowej¹⁷.

Do najważniejszych środków ochrony danych, zapisywanych w księgach rachunkowych programów finansowo-księgowych można zaliczyć¹⁸:

- stosowanie odpornych na zagrożenia nośników danych oraz ich zewnętrzna ochrona;
- systematyczne tworzenie kopii zapasowych zbiorów danych zarejestrowanych na nośnikach komputerowych, mając na uwadze okres, w jakim przechowywanie danych wymagane jest przez poszczególne ustawy;
- stosowanie właściwych rozwiązań organizacyjnych i programowych, mających na celu ochronę danych przed zniszczeniem bądź nieautoryzowanym dostępem.

Oprócz wymogów ustawy o rachunkowości, system finansowo-księgowy powinien spełniać ogólne kryteria bezpieczeństwa przetwarzania informacji (standardy ISO). Wytyczne oceny bezpieczeństwa programów informatycznych są ustalane przez ANSI (*American National Standards Institute*), NITS (*National Institute of Standards and Technology*) oraz IEEE (*Institute of Electrical and Electronic Engineers*). W Polsce szczegółowe warunki dotyczące bezpieczeństwa systemów informatycznych regulują ustawy¹⁹:

- o ochronie informacji niejawnych;
- o ochronie danych osobowych;
- o ochronie tajemnicy państwowej i służbowej;
- o elektronicznych instrumentach płatniczych.

Z uregulowań zawartych w wyżej wymienionych przepisach wynika, że system informatyczny (w tym finansowo-księgowy) powinien być poufny, integralny oraz

¹⁷ T. Cebrowska, op. cit., s. 200.

¹⁸ E. Karwowski, *Plan kont. Zasady rachunkowości z komentarzem*, Wydawnictwo Ad. Drągowski, Warszawa 2001, s. 209.

¹⁹ Ibidem, s. 466-467.

autentyczny, aby spełniać podstawowe kryteria bezpieczeństwa. Z kolei za główne zagrożenia takiego systemu uznaje się: przerwanie (czyli naruszenie poufności), modyfikacje oraz podrobienie. Mimo tych zagrożeń, przechowywanie danych na elektronicznych nośnikach jest bezpieczniejsze i trwalsze, niż zapis na nośnikach papierowych. Niezawodność systemów informatycznych polega na odporności na błędy operatora. System finansowo-księgowy powinien posiadać też wsparcie wytwórcy w postaci: doradztwa technicznego, serwisu oraz okresowej aktualizacji systemu²⁰.

Na rynku istnieje wiele programów finansowych, które różnią się nie tylko zakresem realizowanych funkcji, ale też sposobem zastosowanych zabezpieczeń. Niewątpliwie programem, który spełnia oczekiwania użytkowników w wyżej wymienionych obszarach jest system finansowo-księgowy Symfonia. Finanse i księgowość. Program Symfonia umożliwia prowadzenie ewidencji księgowej, w szczególności: wprowadzanie dokumentów księgowych, szybkie przeglądanie informacji w księgach, odszukiwanie dokumentów źródłowych, szybkie tworzenie różnorodnych sprawozdań²¹. Jest to też program, w którym wykorzystano szerokie spektrum zabezpieczeń dzięki domyślnie wbudowanym opcjom, pozwalającym na minimalizację ryzyka utraty danych. Podstawową formą ochrony danych zgromadzonych w systemie jest wprowadzenie haseł dostępu, które znacznie ograniczają możliwość nieupoważnionej modyfikacji zapisów. Opcja ta wiąże się z przypisywaniem uprawnień poszczególnym użytkownikom, dzięki którym mają oni dostęp tylko do potrzebnych im funkcji. W dużej mierze zmniejsza to ryzyko pomyłki pracownika oraz uniemożliwia im dokonanie zmian w obszarach, do których nie mają prawa dostępu.

Kolejnym sposobem ochrony danych jest funkcja okresowej archiwizacji. „Pozwala ona na sporządzanie dwóch kopii rezerwowych zapisów księgowych, które mogą być przechowywane w dwóch różnych miejscach, chronionych przed dostępem osób niepowołanych”²². Istotne jest również to, że program ma funkcję automatycznego przypominania o konieczności sporządzania kopii bezpieczeństwa.

Podsumowanie

Bezpieczeństwo jest jedną z najważniejszych cech, na jakie należy zwrócić uwagę, wybierając system finansowo-księgowy. Ustalenie odpowiednich środków ochrony nie wymaga ogromnego nakładu pracy, a może minimalizować ryzyko utraty danych, co znajduje też przełożenie na finanse przedsiębiorstwa. Bezpieczeństwo systemów finansowo-księgowych nierozzerwalnie związane jest z bezpieczeństwem całego oprogramowania posiadanego przez daną firmę. Z tego powodu, istotne zna-

²⁰ Ibidem, s. 468

²¹ *Symfonia Finanse i Księgowość. Podręcznik użytkownika. Wersja 2014*, ftp://ftp.sage.com.pl/pub/symfonia/demo/big/AMFK_Podrecznik.pdf [dostęp: 18.05.2014].

²² T. Cebrowska, op. cit., s. 200.

czenie ma wielopoziomowa konstrukcja systemu ochrony danych. Zmniejsza ona ryzyko nieupoważnionej edycji informacji, ich zniszczenia czy też wykorzystania przez osoby trzecie do tego nieupoważnione.

W celu minimalizacji ryzyka z tytułu używania komputerowych systemów finansowo-księgowych przedsiębiorstwa powinny stosować zarówno zabezpieczenia systemowe, jak i organizacyjne. Są one równie ważne i do obydwu przedsiębiorstwo powinno przykładąć ogromną wagę oraz dokładać wszelkich starań, by nie powstały luki w systemie ochrony, dzięki którym dane mogłyby ulec zniszczeniu.

Takim systemem finansowo-księgowym, który spełnia wymogi bezpieczeństwa jest system Symfonia. Program ten posiada różne opcje: tworzenia kopii rezerwowych bazy danych, zapisywania informacji na zewnętrznych nośnikach danych, automatycznego archiwizowania danych, tworzenia wielu użytkowników, co oznacza, iż każdemu można nadać indywidualne uprawnienia oraz zabezpieczyć konta hasłami dostępu.

Literatura

1. Belkaoui A., *Accounting Theory*, HBJ Publishers, San Diego 1985.
2. *Bezpieczeństwo informatyczne – zabezpieczenia dostępu logicznego*, „Rachunkowość” 2004, nr 6, <http://rachunkowosc.com.pl>.
3. Cebrowska T., *Rachunkowość finansowa i podatkowa*, Wydawnictwo Naukowe PWN, Warszawa 2010.
4. Karwowski E., *Plan kont. Zasady rachunkowości z komentarzem*, Wydawnictwo Ad. Drągowski, Warszawa 2001.
5. Michalczuk G. *Zasoby niematerialne jako czynnik wartości przedsiębiorstwa. Luka informacyjna sprawozdawczości finansowej*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2013.
6. Okuń M., *Ochrona danych księgowych oraz systemów informatycznych pod rządami Ustawy o rachunkowości*, [w:] *Technologie informacyjne w finansach i rachunkowość*, N. Siemieniuk, J. Sikorski (red.), Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2003.
7. Ostaszewicz A., *Bezpieczeństwo informatyczne – zabezpieczenia dostępu logicznego*, „Rachunkowość” 2004, nr 6.
8. Rytelwska K., Siemieniuk Ł., *Problematyka zabezpieczenia informacji w zintegrowanych systemach informatycznych*, [w:] *Systemy informatyczne, a funkcjonowanie organizacji gospodarczych*, N. Siemieniuk, J. Sikorski (red.), Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2011.
9. Siemieniuk Ł., *System Symfonia jako przykład zintegrowanego systemu informatycznego w rachunkowości*, „Optimum. Studia Ekonomiczne” 2011, nr 1.
10. *Symfonia Finanse i Księgowość. Podręcznik użytkownika. Wersja 2014*, <ftp://ftp.sage.com.pl>.
11. *Ustawa z dnia 29 września 1994 r. o rachunkowości*, Dz. U. 2013, poz. 613 z późn. zm.