

Karol Schneider

Zagrożenia w systemie informatycznym rachunkowości

Ekonomiczne Problemy Usług nr 87, 740-748

2012

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

KAROL SCHNEIDER
Uniwersytet Szczeciński

ZAGROŻENIA W SYSTEMIE INFORMATYCZNYM RACHUNKOWOŚCI

Wprowadzenie

Współcześnie w różnych dziedzinach działalności ludzkiej coraz częściej używany jest komputer. Urządzenie to ułatwia m.in. sporządzenie dokumentów. Te same jednak cechy, które przesądzają o tym, że komputer jest obecnie coraz powszechniej stosowanym urządzeniem przy sporządzaniu dokumentów, powodują, że stanowi on równocześnie jeden z najgroźniejszych instrumentów wykorzystywanych przy popełnianiu przestępstwa fałszowania dowodów księgowych.

Artykuł jest poświęcony prezentacji zagrożeń, które mogą wystąpić w rachunkowości finansowej i finansowo-księgowej w przedsiębiorstwie. Zagrożenia dla systemu informatycznego rachunkowości można podzielić według różnych kryteriów. Przedstawiono też przepisy prawa bilansowego, które stawiają określone wymagania programom finansowo-księgowym.

System informatyczny rachunkowości jest elementem systemu informacyjnego organizacji, obejmującym zadania rachunkowości, jej funkcje i zasoby danych; składają się na niego dwa główne człony: infrastruktura technologiczna oraz część bezpośrednio wykorzystywana przez użytkowników, nazywana aplikacją.

W skład aplikacji wchodzi ogół lub część zasobów danych rachunkowości, które tradycyjnie nazywane są księgami rachunkowymi, oraz działające na zbiorach tych danych oprogramowanie ukierunkowane na rozwiązywanie problemów rachunkowości.

1. Problemy rachunkowości informatycznej

Istotnym problemem jest możliwość popełnienia przestępstwa za pomocą komputera. Przestępstwo fałszowania dowodów księgowych można ująć w dwóch aspektach. Po pierwsze jako komputerowe fałszerstwo dokumentów w sytuacji, gdy komputer, oprogramowanie i peryferia stanowią narzędzia do fałszowania dokumentów klasycznych. Po drugie jako fałszerstwo dokumentów elektronicznych, polegające na wprowadzaniu zmian w utworzonych i przyjętych dokumentach elektronicznych (księgi handlowe, podatkowe, ewidencje magazynowe) lub też w innych elektronicznych nośnikach informacji.

Fałszowanie dokumentów elektronicznych jest przestępstwem trudnym do wykrycia, gdyż istnieje możliwość tworzenia nieokreślonej liczby kopii, a także wprowadzania niezauważalnych zmian. Niektóre działania przestępcze nie mogą być wykazane, ponieważ nie ma zauważalnych dowodów ich istnienia. Dowody te zostały usunięte lub dotarcie do nich jest bardzo skomplikowane.

Wykorzystanie technik komputerowych w rachunkowości ma wiele zalet, takich jak np. szybkie przetwarzanie informacji, jednoczesny dostęp wielu użytkowników do informacji, dostęp do danych bez konieczności obecności w jednostce gospodarczej oraz zmniejszanie objętości archiwizowanych danych. Jednak te zalety mogą być zniweczone ze względu na fakt istnienia wielu zagrożeń dla systemu informatycznego księgowości. Zagrożenia można kwalifikować według następujących kryteriów¹:

1. Ze względu na źródło mogą być zagrożenia:
 - wewnętrzne, na które jednostka ma wpływ, wśród nich wyróżnia się zagrożenia:
 - organizacyjne, wynikające z nieprawidłowej organizacji jednostki,
 - technologiczne, będące następstwem błędów technologicznych,
 - zewnętrzne, pochodzące z otoczenia jednostki gospodarczej.
2. Ze względu na celowość działań mogą być zagrożenia:
 - przypadkowe (losowe),
 - celowe (umyślne).
3. Ze względu na rodzaj zagrożenia mogą być zagrożenia w stosunku do:
 - oprogramowania,
 - sprzętu.
4. Ze względu na wynik zagrożenia można mówić o:
 - całkowitej utracie danych,
 - kradzieży informacji (wycieku danych),

¹ W. Krawiec, D. Kubiak, *Rodzaje zagrożeń dla systemów informatycznych rachunkowości*, materiały z Konferencji Naukowej Uniwersytetu Szczecińskiego i Akademii Rolniczej w dniach 26-29.05.2006, Szczecin 2006, s. 146–150.

- ingerencji w przetwarzane dane.

Zagrożenia organizacyjne mogą wynikać z wyboru nieodpowiedniego systemu. System finansowo-księgowy powinien spełniać wymogi prawa bilansowego, które dotyczą m.in.:

- zakresu stosowania rozwiązań przewidzianych w ustawie o rachunkowości,
- dokumentacji przyjętych zasad rachunkowości,
- ksiąg rachunkowych,
- wprowadzania zapisów w sposób trwały, chroniący przed modyfikacją lub zniszczeniem zapisów,
- poprawiania błędów w zaksięgowanych dokumentach przez storno (czarne lub czerwone),
- treści dowodów księgowych.

Obowiązujące prawo bilansowe dokładnie precyzuje zakres danych na wejściu oraz informacji wyjściowych, które muszą być emitowane na potrzeby odbiorców zewnętrznych. Połączenie odpowiedniego oprogramowania, mocy obliczeniowej komputerów oraz przeszkolonego personelu może znacząco usprawnić i przyspieszyć pracę służb finansowo-księgowych. Powszechność stosowania elektronicznego systemu przetwarzania danych księgowych niesie pewne niebezpieczeństwa, które mogą być zagrożeniem dla zasady wiernego i rzetelnego obrazu jednostki gospodarczej. W związku z tym ustawa o rachunkowości wprowadza następujące warunki, które muszą być spełnione przy informatycznym systemie przetwarzania danych i dotyczą:

- zbiorów danych składających się na księgi rachunkowe,
- oprogramowania stosowanego do prowadzenia rachunkowości,
- dokumentów księgowych sporządzanych w formie elektronicznej,
- dokumentacji systemów informatycznych rachunkowości,
- zasad ochrony danych.

Prawo bilansowe stanowi, że księgi rachunkowe obejmują²: dziennik, księgę główną, księgi pomocnicze, zestawienie obrotów i sald kont księgi głównej, zestawienie sald kont pomocniczych oraz wykaz składników aktywów i pasywów (inventarz). W tradycyjnej formie zapisów ksiąg rachunkowych przytoczona definicja jest zgodna ze stanem faktycznym. Forma komputerowa jest jednak inna. Z tego względu prawo bilansowe za równoważne z tradycyjnymi księgami rachunkowymi uważa zasoby informacyjne w formie oddzielnych komputerowych zbiorów danych, bazy danych lub wyodrębnionych jej części, bez względu na miejsce powstania i przechowywania. Księgi rachunkowe mogą więc mieć postać struktur danych zorganizowanych w pliki, które są tworzone na dysku twardym komputera. Warunkiem utrzymania ksiąg w takiej formie jest jednak możliwość uzyskania czytelnych

² Ustawa z dnia 29 września 1994 r. o rachunkowości, DzU 2009, nr 152, poz. 1233, z późn. zm.

informacji dotyczących ich treści. Dlatego jednostka gospodarcza musi dysponować nie tylko plikami składającymi się na księgi rachunkowe, lecz także oprogramowaniem, które informacje tego typu tworzy, odczytuje oraz przetwarza do postaci wydruku³.

2. Wymagania stawiane programom finansowo-księgowym

Przepisy prawa bilansowego stawiają określone wymagania programom finansowo-księgowym, obsługującym sferę rachunkowości w jednostce gospodarczej. Ustawodawca zwraca uwagę na konieczność zachowania ciągłości zapisów w księgach rachunkowych oraz wymóg określenia osoby odpowiedzialnej za treść każdego zapisu. Zachowanie ciągłości oznacza automatyczne, kolejne numerowanie poszczególnych zapisów dziennika (lub dzienników częściowych), aby nie były możliwe żadne późniejsze dopiski zmieniające kolejność zapisów już dokonanych. Składnikiem zapisu księgowego powinien być też unikalny kod (identyfikator) osoby, która wprowadza dany zapis do komputera.

Zgodnie z art. 24 ust. 4 pkt 3 ustawy o rachunkowości stosowane oprogramowanie ma zapewnić kompletność zbiorów systemu rachunkowości. Każdy zapis dziennika powinien znaleźć się w księdze głównej oraz ewentualnie na kontach ewidencji analitycznej. Użytkownik systemu musi mieć możliwość kontroli parametrów przetwarzania danych.

Dodatkowe wymagania (zgodnie z art. 12 ust. 5 ustawy o rachunkowości) są także stawiane wydrukowi pochodzącym z informatycznych systemów rachunkowości. Poszczególne strony wydruków powinny być automatycznie numerowane z oznaczeniem strony pierwszej i ostatniej.

Według prawa bilansowego równoważną z wydrukiem formą uzyskiwania informacji co do treści ksiąg rachunkowych jest przeniesienie danych na inny komputerowy nośnik, jeżeli tylko gwarantuje on trwałość zapisu.

3. Zagrożenia w systemie rachunkowości

Większa liczba zagrożeń może wystąpić zarówno już w fazie opracowania oraz tworzenia systemu na potrzeby danej jednostki gospodarczej, jak i podczas jego wykorzystania. Błędne skonfigurowanie systemu, ustalenie błędnych parametrów, np. rozliczenia kosztów, może spowodować, że wygenerowane automatycznie przez system dowody księgowe będą niezgodne z rzeczywistością.

³ A. Bujak, *Specyfika rachunkowości prowadzonej przy użyciu komputera*, Ogólnopolski Zjazd Katedr Rachunkowości, Toruń 2003, s. 96–102.

Zagrożeniem dla systemów informatycznych rachunkowości jest możliwość nadmiernej ingerencji człowieka w działanie systemów informatycznych. Osoby korzystające z systemów mają możliwość poznania słabych stron systemów i procedur kontrolnych, a tym samym mogą zmieniać programy lub dane już podczas ich przetwarzania⁴.

Ponadto zbiory danych archiwizowanych na elektronicznych nośnikach łatwo mogą być przenoszone, a przez to zagrożone kradzieżą przetworzonych danych. Każdy użytkownik systemu ma dostęp do wielu danych będących źródłem informacji o kontrahentach, o pracownikach itp. Dane te mogą być przedmiotem zainteresowania osób trzecich i nierzadko stają się przedmiotem przestępstwa.

Zapewnienie właściwej ochrony zbiorów systemu rachunkowości wymaga więc zabezpieczenia nie tylko samego oprogramowania i danych, lecz także sprzętu komputerowego.

Ustawa nakazuje stosowanie wyłącznie odpornych na zagrożenia nośników danych, nie określając ich jednak dokładnie. Zapis taki oznacza, że to kierownik jednostki, biorąc pod uwagę poziom techniki informatycznej w przedsiębiorstwie oraz posiadane środki finansowe, musi decydować o zastosowaniu konkretnych nośników danych spośród np. taśm, dysków twardych czy płyt CD jednokrotnego lub wielokrotnego zapisu.

Ochrona zewnętrzna sprzętu komputerowego i nośników danych wiąże się z ich zabezpieczeniem przed dostępem osób niepowołanych a także zdarzeniami losowymi (zalanie, pożar), jeśli w ich wyniku mogłoby dojść do fizycznego uszkodzenia lub utraty poszczególnych podzespołów wchodzących w skład komputera oraz dysków lub taśm stanowiących pamięci zewnętrzne. Sprzęt wykorzystywany do prowadzenia rachunkowości powinien być więc przechowywany w zamkniętych pomieszczeniach zabezpieczonych przed kradzieżą, wyposażonych w urządzenia przeciwpożarowe, listwy przeciwprzepięciowe oraz awaryjne zasilacze, które pozwalają na bezpieczne eksploataowanie sprzętu komputerowego.

Rozwiązania organizacyjne powinny regulować dostęp do sprzętu i pomieszczeń oraz ustalać warunki, jakie powinny spełniać pomieszczenia ze sprzętem w celu ochrony danych. Sposób i częstotliwość archiwizacji danych oraz formy przechowywania kopii zapasowych powinny być również sprecyzowane. Wśród istotniejszych rozwiązań w przedmiocie procedur organizacyjnych należy wymienić⁵:

- określenie przez administratora systemu praw i obowiązków każdego użytkownika w zakresie wprowadzania, modyfikowania i usuwania danych w programie,

⁴ E. Dudek, *Zagrożenia występujące w środowisku informatycznym rachunkowości*, „Monitor Rachunkowości i Finansów” 2003, nr 7–8, s. 46–47.

⁵ K. Schneider, *Błędy i oszustwa w dokumentach finansowo-księgowych*, PWE, Warszawa 2007, s. 81–83.

- wyznaczenie częstotliwości tworzenia rezerwowych kopii zbiorów danych oraz wskazanie miejsca ich przechowywania (względny bezpieczeństwa wymagają, aby archiwizowane dane nie znajdowały się w tym samym pomieszczeniu, w którym przechowywane są zbiory podstawowe),
- określenie zasad bieżącej antywirusowej kontroli nośników danych,
- wskazanie miejsca przechowywania wersji instalacyjnej programu finansowo-księgowego (ze względów bezpieczeństwa również powinno ono znajdować się poza pomieszczeniem, gdzie odbywa się codzienna praca z programem),
- prowadzenie szkoleń dotyczących obsługi oprogramowania i sprzętu komputerowego dla pracowników będących użytkownikami systemu,
- zachowanie tajemnicy służbowej (ochrona haseł dostępu oraz zawartości zbiorów komputerowych).

Praktyka wskazuje, że przy prowadzeniu ksiąg rachunkowych za pomocą komputera występuje wiele nieprawidłowości, jak⁶:

- brak w dokumentacji jednostki opisów wykazanych w art. 10 ustawy o rachunkowości, a dotyczących informatycznego systemu przetwarzania danych zastosowanego przez jednostkę,
- formalne traktowanie dziennika wyrażające się m.in. w jego sporządzeniu po zaksięgowaniu operacji lub niesporządzeniu go wcale,
- stosowanie dzienników częściowych bez sporządzania dziennika zbiorczego,
- brak ciągłości zapisów oraz jednoznacznych powiązań między księgami,
- niekompletność zapisów księgowych oraz elementów opisu określających daną księgę i wykazywanych w niej informacji,
- brak zgodności sum obrotów dziennika z zestawieniem obrotów i sald oraz kont księgi głównej,
- rozbieżności między saldami kont księgi głównej a sumą sald ksiąg pomocniczych,
- wpisywanie na tabulogramach i wydrukach dowolnej daty ich sporządzenia,
- dokonywanie zmian w zapisach księgowych w zamkniętych okresach sprawozdawczych,
- stosowanie przemiennie zapisów sum dodatnich i ujemnych.

Należy jednak zauważyć, że współczesne zdobycze technologii informatycznej mogą powodować dla rachunkowości wiele zagrożeń, do których niewątpliwie można zaliczyć możliwość nieprzestrzegania zasady dokonywania zapisów w ewidencji księgowej w sposób chronologiczny i systematyczny. Technika informatycz-

⁶ R. Ozyński, *Prowadzenie ksiąg rachunkowych za pomocą komputera*, II Doroczna Konferencja Krajowej Izby Biegłych Rewidentów, Jachranka, 22–24 listopada 2001, s. 201.

na, pozwalająca na wielokrotne wpisywanie i wymazywanie danych, niestety takie możliwości stwarza, mimo prawnych zakazów⁷.

Dowodem na to jest fakt, że wręcz praktyką wśród księgowych stało się zapisywanie dokumentów w systemach komputerowych do bufora (tymczasowo) przez cały rok obrotowy, a nie do ksiąg (zapis trwałe).

Do nowych zagrożeń związanych z zastosowaniem narzędzi informatycznych można zaliczyć zagrożenia dotyczące bezpieczeństwa danych. Dostęp osób nieuprawnionych do danych systemu informatycznego lub też naruszenie zasad bezpieczeństwa danych może mieć bezpośrednio lub pośrednio ujemny wpływ na sytuację finansową jednostki. Do tego typu zagrożeń bezpośrednich można zaliczyć:

- oszustwa polegające na włamaniu do systemu i nieuprawnioną manipulację danymi,
- awarię systemu informatycznego skutkującą przestojami działalności operacyjnej przedsiębiorstwa,
- stratę części danych i koszty związane z ich odtwarzaniem.

Do zagrożeń pośrednio wpływających na sytuację jednostki można zaliczyć:

- dostęp osób nieuprawnionych do danych dotyczących klientów, który może negatywnie odbić się na reputacji jednostki gospodarczej,
- nieuprawnione funkcjonowanie systemu, które może ujemnie odbić się na operacyjnej efektywności jednostki gospodarczej.

Ostatnią kwestią regulującą zasady bezpieczeństwa danych systemu rachunkowości jest konieczność stosowania takich procedur programowych i organizacyjnych, które chronią oprogramowanie oraz zbiory danych przed nieupoważnionym dostępem lub zniszczeniem. Do procedur programowych zaliczyć należy przede wszystkim nadawanie haseł dostępu wszystkim użytkownikom programu. Zabezpieczenia tego rodzaju mogą być stosowane na poziomie:

- komputera, jeśli przed uruchomieniem systemu operacyjnego wprowadzane jest hasło,
- systemu informatycznego, gdy rozpoczęcie pracy z programem wymaga podania hasła,
- wybranych funkcji systemu informatycznego, jeżeli pewne działania wykonywane przez program zastrzeżone są dla konkretnych, znających odpowiednie hasło użytkowników.

Stosowane procedury organizacyjne mają zapewnić taki sposób organizacji pracy użytkowników systemu informatycznego, który będzie gwarantować bezpieczeństwo danych. Wybór stosowanych metod pozostaje w gestii kierownictwa danej jednostki gospodarczej.

⁷ M. Andrzejewski, *Nowoczesne systemy informatyczne wspomagające rachunkowość małych i średnich przedsiębiorstw*, WSPiM, Chrzanów 2003, s. 10–104.

Podsumowanie

Racjonalne gospodarowanie musi mieć odpowiednią bazę informacyjną. System informacyjny spełnia zaś swą rolę, gdy jest dobry jakościowo, wiarygodny. Od systemu tego wymaga się, aby umożliwił on:

- trwały dobór informacji z pełnego ich zbioru,
- właściwą ich ocenę według istotnego znaczenia,
- właściwe łączenie informacji odpowiednio do ich wzajemnego powiązania.

Wszystkie te postulaty znajdują się w obszarze czynników budujących wiarygodność systemu informacyjnego. W przypadku rachunkowości jako pragmatycznego systemu informacyjno-kontrolnego ta wiarygodność ma najistotniejsze znaczenie.

Literatura

1. Andrzejewski M., *Nowoczesne systemy informatyczne wspomagające rachunkowość małych i średnich przedsiębiorstw*, WSPiM, Chrzanów 2003.
2. Bujak A., *Specyfika rachunkowości prowadzonej przy użyciu komputera*, Ogólnopolski Zjazd Katedr Rachunkowości, Toruń 2003.
3. Dudek E., *Zagrożenia występujące w środowisku informatycznym rachunkowości*, „Monitor Rachunkowości i Finansów” 2003, nr 7–8.
4. Krawiec W., Kubiak D., *Rodzaje zagrożeń dla systemów informatycznych rachunkowości*, materiały z Konferencji Naukowej Uniwersytetu Szczecińskiego i Akademii Rolniczej w dniach 26–29.05.2006, Szczecin 2006.
5. Ożyński R., *Prowadzenie ksiąg rachunkowych za pomocą komputera*, II Doroczna Konferencja Krajowej Izby Biegłych Rewidentów, Jachranka, 22–24 listopada 2001.
6. Schneider K., *Błędy i oszustwa w dokumentach finansowo-księgowych*, PWE, Warszawa 2007.
7. Ustawa dnia z 29 września 1994 roku o rachunkowości, DzU 2009, nr 152, poz. 1233, z późn. zm.

THREATS OF THE ACCOUNTING INFORMATION SYSTEM

Summary

The purpose of the article is to answer the question how a wrong configuration of the accounting information system should be avoided. The author focused especially on

circumstances where the use of false parameter, for example in the calculation of costs, can lead to a situation, that the obtained by the automated system values, do not match the real ones.

Translated by Kamila Schneider