STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 158

158/2017
s. 61–73

Szkoła Główna Handlowa w Warszawie
Oficyna Wydawnicza SGH
kolegia.sgh.waw.pl

Mariusz Sokołek
Katolicki Uniwersytet Lubelski Jana Pawła II

Zewnętrzna obsługa księgowa a polityka rachunkowości w zakresie zabezpieczenia dostępu do danych ksiąg rachunkowych

Streszczenie

Ostatnie lata to era szybkiego postępu technologicznego – szczególnie w sferze teleinformatyki. Nowoczesne rozwiązania informatyczne wykorzystywane są również w biznesie, a za tym też w rachunkowości. Nowoczesne technologie przyczyniają się do m.in. obniżenia kosztów, łatwości i szybkości przetwarzania danych. Wiele czynności wykonywanych jest w cyberprzestrzeni. Jednak poza pozytywnymi stronami rozwoju technologii informatycznych zauważalne są zagrożenia w postaci niepożądanych udostępnień danych księgowych, ich kasowania lub modyfikowania. W artykule poruszono problem zabezpieczenia danych księgowych przed niewłaściwym dostępem i wykorzystaniem, w sytuacji obsługi rachunkowej przedsiębiorstwa świadczonej przez podmiot zewnętrzny. Dokonano przeglądu aktów prawnych regulujących kwestię ochrony dostępu do danych z ksiąg rachunkowych oraz stanowisk w tej materii prezentowanych przez przedstawicieli nauki. Przedstawiono realne zagrożenia oraz sposoby zabezpieczenia się przed cyberatakami w sferze rachunkowości.

Słowa kluczowe: rachunkowość, ochrona danych, bezpieczeństwo danych, polityka rachunkowości, cyberprzestrzeń, dane księgowe
Kod klasyfikacji JEL: M480

1. Wprowadzenie

Rozwój technologii informatycznych zmienił w ostatnich latach podejście do obsługi rachunkowej jednostek. Wiele firm, szczególnie z sektora małych i średnich przedsiębiorstw, decyduje się na obsługę księgową w ramach świadczenia usług przez podmiot zewnętrzny – biuro rachunkowe. Według badania Small Business DNA 51% firm mikro i małych korzysta z obsługi księgowej świadczonej przez biuro rachunkowe. Tylko 12% firm z sektora mikro i małych zatrudnia księgowego, a aż 37% firm prowadzi księgowość samodzielnie[1]. Na obsługę księgową decydują się również duże jednostki i międzynarodowe korporacje – korzystają one z usług centrów finansowych dedykowanych obsłudze jednej sieci lub z biur ogólnodostępnych. Do najczęstszych powodów rezygnacji z prowadzenia rachunkowości w siedzibie jednostki na rzecz obsługi świadczonej przez wyspecjalizowane biuro rachunkowe wymienia się:

- ograniczenie kosztów związanych z:
  - zatrudnieniem,
  - rotacją pracowników,
  - nieobecnością kadry księgowej (choroby, urlopy),
  - sprzętem IT,
  - dostępem do fachowej i bieżącej wiedzy rachunkowo-podatkowej;
- elastyczność w kontaktach;
- dostęp do nowych technologii;
- ograniczenie odpowiedzialności.

Kierownik jednostki powinien mieć jednak świadomość, że decyzja o skorzystaniu z usług biura rachunkowego może rodzić, poza korzyściami z zakresu obniżenia kosztów, pewne zagrożenia, związane m.in. z dostępem do danych ewidencjonowanych w księgach rachunkowych. Należy pamiętać, że oprócz zapisów księgowych osoby zajmujące się obsługą rachunkową siłą rzeczy mają często nieograniczony dostęp do dowodów źródłowych (faktur, wyciągów bankowych, raportów kasowych) oraz sprawozdań finansowych i innych raportów.

Niniejszy artykuł przedstawia stan obecny, wynikający z regulacji prawnych w zakresie ochrony dostępu do zbioru danych księgowych oraz jego charakterystykę

[1] inFakt, *Księgowy – w biurze czy w chmurze?*, https://www.infakt.pl/front/files/InFakt_Dzien_Ksiegowego.pdf, dostęp 8.11.2016.

w literaturze naukowej. Autor zwraca uwagę na niedostosowanie przepisów ustaw do problemu dostępu do danych finansowych jednostek. W artykule zawarto też wnioski, praktyczne wskazówki oraz rekomendacje z racji zajmowanego przez autora stanowiska głównego księgowego oraz doświadczenia nabytego podczas prowadzenia biura rachunkowego.

Literatura fachowa dotycząca problemu polityki rachunkowości (do jej opracowania zobowiązuje ustawa o rachunkowości) wymienia zwykle obowiązki, jakie ciążą na kierowniku jednostki, i skupia się na sposobach, metodach wyceny oraz na charakterystyce zakładowego planu kont, ale nie daje kierownikom jednostki rekomendacji czy wzorców ochrony dostępu do danych księgowych jednostki. Kierownik, kierując się zaufaniem i brakiem świadomości zagrożeń płynących z cyberataków, może pomijać ten fakt w organizacji rachunkowości i nie opracować skutecznych procedur. Co więcej, dostęp do zasobów informatycznych nie musi wynikać jedynie z działania hakerów. Osoby związane z jednostką, np. pracownicy, za sprawą dostępu do danych mogą udostępniać nieuprawnionym osobom trzecim dane pochodzące z systemu rachunkowości w postaci bazy kontrahentów, stosowanych cen i marż, stanów magazynowych i wiele innych informacji. W tym zakresie dokonano przeglądu zarówno aktów prawnych, norm oraz standardów, jak i literatury fachowej z przedmiotu problemu. Literatura z tego obszaru jest bardzo ograniczona. Problem bezpieczeństwa danych zawarty jest jedynie w komentarzach do ustawy o rachunkowości. Tu dokonano krytycznej analizy treści literatury. Jedynie normy prawne oraz standardy dość enigmatycznie zobowiązują do opracowania procedur, które są wewnętrzną decyzją kierownika jednostki. Analiza dostępnej literatury, niewykazana w odrębnej pozycji poświęconej temu zagadnieniu, stanowi jednak dość ważne w obecnych czasach wyzwanie dla przedstawicieli nauki, by zdiagnozowali problem, a następnie przekazali niezbędny materiał jednostkom.

Z uwagi na tematykę konferencji Forum Rachunkowości w SGH no 3 *Cyberprzestrzeń a rachunkowość* i słuszne zwrócenie uwagi nie tylko na *stricte* naukowy charakter problemu, lecz także na jego naturę praktyczną, płynącą z codziennej praktyki biznesu, opisywany temat wydaje się niezmiernie ważny, choć w praktyce bywa niezauważalny i bagatelizowany, przynajmniej do momentu ujawnienia informacji o niekontrolowanym dostępie do niejawnych danych przedsiębiorcy.

2. Polityka rachunkowości a ochrona danych księgowych

W myśl ustawy o rachunkowości[2] (art. 10) na kierowniku jednostki spoczywa obowiązek opracowania zasad (polityki) rachunkowości. Obejmują one co najmniej:

1) określenie roku obrotowego i wchodzących w jego skład okresów sprawozdawczych;
2) metody wyceny aktywów i pasywów oraz ustalania wyniku finansowego;
3) sposób prowadzenia ksiąg rachunkowych, w tym co najmniej:
   a) zakładowego planu kont, ustalającego wykaz kont księgi głównej, przyjęte zasady klasyfikacji zdarzeń, zasady prowadzenia kont ksiąg pomocniczych oraz ich powiązania z kontami księgi głównej,
   b) wykazu ksiąg rachunkowych, a przy prowadzeniu ksiąg rachunkowych przy użyciu komputera – wykazu zbiorów danych tworzących księgi rachunkowe na informatycznych nośnikach danych z określeniem ich struktury, wzajemnych powiązań oraz ich funkcji w organizacji całości ksiąg rachunkowych i w procesach przetwarzania danych,
   c) opisu systemu przetwarzania danych, a przy prowadzeniu ksiąg rachunkowych przy użyciu komputera – opisu systemu informatycznego, zawierającego wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, wraz z opisem algorytmów i parametrów oraz programowych zasad ochrony danych, **w tym w szczególności metod zabezpieczenia dostępu do danych i systemu ich przetwarzania**, a ponadto określenie wersji oprogramowania i daty rozpoczęcia jego eksploatacji;
4) **system służący ochronie danych i ich zbiorów, w tym dowodów księgowych, ksiąg rachunkowych i innych dokumentów stanowiących podstawę dokonanych w nich zapisów**.

Ponadto rozdział 8 ustawy o rachunkowości poświęcony jest ochronie danych. Przepisy te zobowiązują kierownika jednostki do opracowania zasad trwałości i archiwizacji danych. Z kolei w art. 75 ustawy o rachunkowości znajduje się dość ogólne i lakoniczne stwierdzenie, że udostępnienie osobie trzeciej zbiorów lub ich części:

1) do wglądu na terenie jednostki – wymaga zgody kierownika jednostki lub osoby przez niego upoważnionej,

[2] Ustawa z dnia 29 września 1994 r. o rachunkowości, DzU z 2016 r., poz. 1047.

2) poza siedzibą zarządu (oddziału) jednostki – wymaga pisemnej zgody kierownika jednostki oraz pozostawienia w jednostce potwierdzonego spisu przejętych dokumentów.

Literatura fachowa również nie omawia kwestii opracowania procedur przekazywania i wglądu do danych księgowych jednostki. W komentarzu do ustawy o rachunkowości A. Helin[3] odnosi ustalenia ustawy w tym zakresie raczej do udostępnienia zbiorów danych osobom trzecim w kontekście przeprowadzenia badania sprawozdania finansowego biegłemu rewidentowi, o czym stanowi art. 67 ustawy o rachunkowości. Osobami trzecimi w myśl ustawy są też przedstawiciele organów kontrolnych, którzy czynności kontrolnych mogą dokonywać w siedzibie jednostki lub poza nią. Ustawa narzuca obowiązek pisemnej zgody kierownika na udostępnienie dokumentów księgowych wraz ze spisem przejętych dokumentów[4]. G. Idzikowska w komentarzu do ustawy o rachunkowości[5] stwierdza zaś, że „w jednostce musi być opracowana i przestrzegana procedura udostępniania zasobów informacyjnych, która uwzględnia także inne, poza ustawą o rachunkowości, przepisy prawne (np. ustawę o ochronie danych osobowych czy przepisy dotyczące informacji niejawnych lub informacji stanowiących tajemnicę państwową)" i zauważa jedynie aspekt obowiązku z tytułu innych ustaw, które przytoczono w cytacie. Niemniej brakuje odniesienia do udostępnienia przedstawicielom biura rachunkowego zbioru danych rozumianych – w myśl art. 10 ust. 4 ustawy o rachunkowości – nie tylko jako księgi rachunkowe, lecz także jako dowody księgowe czy dokumenty inwentaryzacyjne. Ten sam zakres wskazują inni autorzy komentarzy do rachunkowości: R. Seredyński i K. Szaruga[6].

Wskazać należy też na stanowisko Komitetu Standardów Rachunkowości w sprawie niektórych zasad prowadzenia rachunkowości[7], które zobowiązują kierownika jednostki do efektywnego, bieżącego sprawowania nadzoru nad usługami świadczonymi przez podmiot, zajmujący się obsługą księgową. Może to się przejawiać

[3] A. Helin, *Ustawa o rachunkowości. Komentarz*, wyd. 6, C.H. Beck, Warszawa 2014, s. 716.

[4] Ibidem.

[5] *Ustawa o rachunkowości. Komentarz*, red. E. Walińska, wyd. 4, Wolters Kluwer, Warszawa 2016.

[6] R. Seredyński, K. Szaruga, *Komentarz do ustawy o rachunkowości*, Wydawnictwo ODDK, Gdańsk 2016, s. 899.

[7] Komunikat nr 10 Ministra Finansów z dnia 18.05.2010 r. w sprawie ogłoszenia uchwały Komitetu Standardów Rachunkowości w sprawie przyjęcia stanowiska Komitetu w sprawie niektórych zasad prowadzenia ksiąg rachunkowych, Dziennik Urzędowy Ministra Finansów nr 6, poz. 26, http://www.mf.gov.pl/documents/764034/1194473/DZIENNIK+URZ%C4%98DOWY+MINISTRA+FINANS%C3%93W+NR+6+Z+DNIA+24+CZERWCA+2010+R, dostęp 9.11.2016.

poprzez kontrolę zapisów księgowych (również *online*), okresowe raportowanie lub raportowanie na żądanie. Standard wskazuje, że kierownik jednostki powinien kontrolować kwalifikacje osób faktycznie wykonujących czynności ewidencyjne. Biegły rewident w jednostkach, które na podstawie ustawy o rachunkowości podlegają badaniu przez biegłego rewidenta – zgodnie z ust. 76 pkt f Krajowego Standardu Rewizji Finansowej nr 1[8] – w raporcie dotyczącym badania zobowiązany jest do oceny stosowanych metod zabezpieczenia dostępu do danych i systemu ich przetwarzania za pomocą komputera. W związku z tym w jednostkach niepodlegających badaniu czynności te wykonuje kierownik jednostki.

3. Obszary zagrożenia dostępu do danych w kontekście zewnętrznej obsługi księgowej

Kierownik jednostki w związku z zawarciem umowy z zewnętrznym przedsiębiorcą świadczącym usługi księgowe ma podwójny obowiązek ochrony przed dostępem do danych finansowych. Przede wszystkim powinien dołożyć starań, by osoby bezpośrednio związane z jednostką (współwłaściciel, osoby współpracujące, pracownicy, zleceniobiorcy) i posiadające dostęp do danych miały precyzyjnie określony zakres czynności związanych z tworzeniem i przetwarzaniem danych księgowych oraz dokumentów źródłowych. Zadania i ograniczony dostęp do danych może dotyczyć różnych osób, np. fakturzystów, magazynierów osób zajmujących się przygotowywaniem płatności i obsługujących konta bankowe czy kasjerów. Należy w tym miejscu podkreślić, że w dobie możliwości technologicznych wiele jednostek decyduje się na dostęp do programów magazynowych, fakturowych, kont bankowych za pomocą łączy internetowych i platform *online*. Z jednej strony jest to podyktowane szybkością i wygodą dostępu do bieżących czynności, np. wystawiania faktury, weryfikowania stanów magazynowych, czy – w razie nagłej potrzeby – możliwością dokonania płatności w systemie bankowym. Osoba zarządzająca jednostką powinna mieć świadomość, że taki dostęp pozwala na przegląd danych, a nawet ich kopiowanie z dowolnego miejsca w dowolnym czasie.

W kontekście obsługi outsourcingowej biuro rachunkowe często oferuje zintegrowany system, pozwalający na jednoczesny dostęp do dokumentów źródłowych

[8] Załączniki do uchwały nr 1608/38/2010 Krajowej Rady Biegłych Rewidentów z dnia 16 lutego 2010 r.

powstających w działalności operacyjnej przedsiębiorstwa oraz do modułu finansowo-księgowego jednostki – zwykle w formie dostępu *online*. Komunikacja w tych obszarach jest dwukierunkowa. To daje kolejne możliwości wglądu i udostępniania danych osobom trzecim.

Należy pokreślić, że logowanie *online* za pomocą łączy internetowych daje możliwość zapisywania loginu i hasła w pamięci komputera – stanowiska pracy. Stąd rekomendacja, która wymaga opracowania odpowiedniej procedury, by stanowisko komputerowe, z którego dokonywane jest logowanie do systemu, było zabezpieczone odpowiednim hasłem dostępu do systemu operacyjnego stanowiska komputerowego, a przy braku czynności w systemie następowało automatyczne wylogowanie systemu po określonym czasie (stosunkowo krótkim). Zwykła nieuwaga pracownika, który nie wylogował się z systemu, może spowodować odczytanie danych do logowania w systemie finansowo-księgowym. Niezbędne jest też przyporządkowanie określonym pracownikom wyodrębnionego w systemie zakresu czynności i uprawnień. Na przykład kasjer powinien mieć uprawnienia jedynie do obsługi dokumentów kasowych (KP, KW oraz generowanie/księgowanie raportu kasowego), bez dostępu do pozostałych danych.

W przypadku obsługi księgowej przez jednostkę zewnętrzną w celu zabezpieczenia dostępu do danych kierownik powinien być zobowiązany do określenia w umowie łączącej jednostkę z biurem rachunkowym, by każdorazowy dostęp do systemu czy dokumentów księgowych miały jedynie osoby, co do których kierownik jednostki wyraził zgodę.

E. Klamut zwraca uwagę, że centra obsługi finansowej czy biura rachunkowe cechują się dużą rotacją kadr. Problem ten szczególnie dotyczy osób o wysokich kwalifikacjach i mających duży potencjał wiedzy i rozwoju. Poza tym E. Klamut podkreśla, że takie zmiany w zatrudnieniu mogą „zakłócić funkcjonowanie biura i spowodować nierzetelne wykonanie usługi"[9]. Pracownicy biura „nie są emocjonalnie związani ani z biurem, ani z klientem, prace związane z obsługą księgową klienta traktują «taśmowo»"[10]. Zwraca też uwagę na to, że pracownicy słabo wykwalifikowani zwiększają ryzyko błędu. Obsługa kilku, a wielu przypadkach – dużej liczby podmiotów w biurze rachunkowym niesie za sobą ryzyko błędu wywołanego pośpiechem i wymuszoną okresową zmianą obsługiwanych podmiotów. W kontekście dostępu

[9] E. Klamut, *Ryzyko w działalności biur rachunkowych*, „Przedsiębiorczość i Zarządzanie", t. XIII, z. 15, s. 15–16.

[10] Ibidem, s. 59.

i ochrony danych księgowych wykwalifikowana kadra może stwarzać zagrożenie świadomego i zaplanowanego wycieku informacji. Z kolei kadra o niskich kwalifikacjach i jej nieświadomość oraz niefrasobliwość mogą spowodować niekontrolowany dostęp do danych księgowych przez osoby trzecie, zainteresowane takim dostępem. Według badań PwC główne, bo aż 70%, źródła cyberataków w Polsce to pracownicy – ci obecni i już niepracujący[11].

W przypadku prostych prac ewidencyjnych czy segregacyjnych dokumentacji księgowej biura rachunkowe często korzystają ze wsparcia stażystów lub praktykantów. Osoby te okazjonalnie przebywają w biurze, a jednocześnie mogą mieć niekontrolowany i nieograniczony dostęp do wrażliwych danych księgowych, których ujawnienie lub upowszechnienie może wiązać się ze szkodami dla obsługiwanej jednostki. Niepożądane czynności pracowników biur rachunkowych mogą polegać też na świadomym lub nieświadomym niszczeniu (kasowaniu) danych lub ich modyfikacji z poziomu dostępu do zasobów informatycznych, a nawet na udostępnianiu osobom trzecim loginów i haseł dostępu.

Właściciele biur rachunkowych, świadomi tych zagrożeń, muszą wykazać się czujnością i ograniczonym zaufaniem, a co za tym idzie – sprawować odpowiedni nadzór i opracować szczegółowe procedury. Kierownik obsługiwanej jednostki jest jednak pozbawiony jakiejkolwiek kontroli w tym zakresie. To dlatego przezorność i dbałość o bezpieczeństwo jednostki powinno skłonić kierownika do podejmowania czynności kontrolnych.

4. Odpowiedzialność z tytułu utraty lub zmiany danych w księgach rachunkowych

Ustawa o rachunkowości w art. 4 ust. 5 określa, że to kierownik jednostki ponosi pełną odpowiedzialność z tytułu wykonywania obowiązków w zakresie rachunkowości. Z kolei w art. 4 ust. 3 zdefiniowano zakres tej odpowiedzialności. Otóż rachunkowość obejmuje:

1) przyjęte zasady (politykę) rachunkowości,
2) prowadzenie, na podstawie dowodów księgowych, ksiąg rachunkowych, ujmujących zapisy zdarzeń w porządku chronologicznym i systematycznym,

[11] *W obronie cyfrowych granic. Czyli 5 rad, aby realnie wzmocnić firmy przed cyber ryzykiem*, PwC, Warszawa, styczeń 2016, www.pwc.pl/badaniebezpieczenstwa, dostęp 7.11.2016.

3) okresowe ustalanie lub sprawdzanie drogą inwentaryzacji rzeczywistego stanu aktywów i pasywów,
4) wycenę aktywów i pasywów oraz ustalanie wyniku finansowego,
5) sporządzanie sprawozdań finansowych,
6) gromadzenie i przechowywanie dowodów księgowych oraz pozostałej dokumentacji przewidzianej ustawą,
7) poddanie badaniu, składanie do właściwego rejestru sądowego, udostępnianie i ogłaszanie sprawozdań finansowych w przypadkach przewidzianych ustawą.

W kontekście obsługi świadczonej przez podmiot zewnętrzny (biuro rachunkowe) w art. 4 ust. 5 określono, że w przypadku gdy prowadzenie ksiąg rachunkowych zostanie powierzone innej osobie lub przedsiębiorcy (główny księgowy, biuro rachunkowe), pełna odpowiedzialność za rzetelność prezentowanych danych spoczywa na kierowniku jednostki. Oznacza to, że żadna jednostka nie ma możliwości scedowania na inne osoby trzecie odpowiedzialności za wykonywanie ustawy.

W sytuacji, w której mamy do czynienia z kierownictwem wieloosobowym, każdy z przedstawicieli kierownictwa jednostki odpowiada solidarnie wobec jednostki, którą kieruje, za szkodę wyrządzoną działaniem lub zaniechaniem. Nietrudno się domyślić, że kadrze zarządzającej często trudno pogodzić się z obciążeniem z tytułu odpowiedzialności, o której mowa w ustawie o rachunkowości. Obciążenie to polega na stosowaniu kary grzywny lub kary pozbawienia wolności do lat dwóch albo obu tych kar łącznie (art. 77 ustawy o rachunkowości)[12].

Należy też nadmienić, że oprócz kar ustawowych odpowiedzialność może mieć wymiar społeczny, moralny czy etyczny. Dotyczy to w szczególności osób pełniących funkcje księgowego. Dostrzegając ten problem, Międzynarodowa Federacja Księgowych (IFAC) w *Kodeksie zasady etyki zawodowej*[13] zwraca uwagę na misję, jaką ma do wykonania księgowy. Podkreśla się tam nie tylko to, że księgowy ma zaspokoić potrzeby indywidualne pracodawcy lub klienta, lecz także że jego działania przekładają się na interes publiczny. Zgodnie z ogólną koncepcją zawartą w kodeksie:

[12] M. Sokołek, *Zasady odpowiedzialności za rzetelność danych prezentowanych w sprawozdaniu finansowym*, w: *Sprawozdawczość finansowa w systemie wymiany informacji i bezpieczeństwa obrotu gospodarczego*, red. H. Żukowska, M. Zuba-Ciszewska, P. Bolibok, Wydawnictwo KUL, Lublin 2016, s. 83–84.

[13] Międzynarodowa Federacja Księgowych (IFAC), *Kodeks etyki zawodowych księgowych*, tłum. Stowarzyszenie Księgowych w Polsce, 2011, http://www.skwp.pl/files/zg/Kodeks_etyki_IFAC.pdf, dostęp 29.10.2015.

„Zawodowy księgowy postępuje zgodnie z następującymi podstawowymi zasadami:

a) Uczciwość – postępowanie w sposób otwarty i uczciwy we wszystkich powiązaniach zawodowych i gospodarczych.
b) Obiektywizm – dbałość, aby uprzedzenia, konflikty interesów lub niepożądane oddziaływania osób trzecich nie wpływały na osądy o charakterze zawodowym lub gospodarczym.
c) Zawodowe kompetencje i należyta staranność – posiadanie fachowej wiedzy oraz umiejętności zawodowych na poziomie wymaganym dla zapewnienia, że klient lub pracodawca uzyskuje kompetentne, profesjonalne usługi, oparte na najnowszych rozwiązaniach z zakresu wykonywania zawodu, regulacji prawnych i metodologii, a także zachowywanie staranności oraz przestrzeganie odpowiednich standardów technicznych i zawodowych.
d) Zachowanie tajemnicy informacji – przestrzeganie zasady zachowania tajemnicy informacji uzyskanych w wyniku powiązań zawodowych i gospodarczych. W związku z tym zawodowy księgowy nie ujawnia takich informacji stronom trzecim bez odpowiedniego i wyraźnego upoważnienia – chyba że ich ujawnienie wynika z prawnych lub zawodowych uprawnień lub obowiązków – oraz nie wykorzystuje takich informacji dla realizacji swoich osobistych korzyści lub osobistych korzyści stron trzecich.
e) Profesjonalne postępowanie – postępowanie zgodnie z odpowiednimi przepisami prawa i regulacjami oraz unikanie wszelkich działań dyskredytujących zawód"[14].

W celu przeniesienia obciążeń z tytułu odpowiedzialności za jakość ksiąg i sprawozdań finansowych osoby prawne (spółki z ograniczoną odpowiedzialnością, spółki akcyjne i inne osoby prawne), zatrudniając osobę pełniącą w jednostce funkcję głównego księgowego czy dyrektora finansowego, jednocześnie powołują tę osobę na stanowisko członka zarządu.

Komitet Standardów Rachunkowości w uchwale nr 5/10 z dnia 13 kwietnia 2010 r.[15] w pkt. 24 potwierdza, że powierzenie prowadzenia ksiąg rachunkowych podmiotowi zewnętrznemu nie zwalnia kierownika jednostki z odpowiedzialności za wykonywanie obowiązków w zakresie rachunkowości.

[14] Ibidem, s. 4–5.
[15] *Komunikat nr 10...*, op.cit.

5. Podsumowanie

Sektor małych i średnich przedsiębiorstw staje się coraz częstszym obiektem cyberataków, które mogą mieć różny wymiar. Przede wszystkim są to ataki hakerów, polegające na włamaniu się do zasobów danych informatycznych, ich ujawnieniu, kopiowaniu, kasowaniu lub modyfikowaniu. Cyberprzestrzeń to również dostęp do zasobów informatycznych wewnątrz jednostki. Właściwy, tzn. kontrolowany i świadomy nadzór nad dostępem do baz danych, staje się czynnością priorytetową dla właściciela (kierownika) przedsiębiorstwa. Utrata, ujawnienie czy modyfikacja danych mogą zakłócić funkcjonowanie jednostki i generować nieoczekiwane straty. O ile jednak kierownik przedsiębiorstwa ma wpływ na zarządzanie dostępem do własnych danych finansowo-księgowych, o tyle w przypadku obsługi świadczonej przez podmiot zewnętrzny (biuro rachunkowe) staje się to nieosiągalne, a nawet niemożliwe. Klient biura powinien więc w umowie zapisać stosowne wymagania, tak aby w przypadku niepożądanych działań w cyberprzestrzeni mógł dochodzić roszczeń na drodze sądowej z powództwa cywilnego. Proces dochodzenia praw może być niełatwy, długotrwały oraz generować dodatkowe koszty fachowej obsługi prawnej. Prawidłowe działanie sektora usług finansowo-księgowych niewątpliwie ma więc wpływ na efektywne działanie szczególnie sektora małych i średnich przedsiębiorstw – głównych klientów biur rachunkowych. Stąd pozostawienie tego sektora bez precyzyjnych uregulowań prawnych, nadzoru i wsparcia (również w kontekście niewłaściwego zarządzania przepływem i dostępu do informacji finansowo-księgowych) może mieć negatywny wpływ na funkcjonowanie przedsiębiorstw.

Właściwe wydaje się rozwinięcie i sprecyzowanie w ustawie o rachunkowości zasad przetwarzania zasobów danych ksiąg rachunkowych (szczególnie w przypadku obsługi księgowej przez podmioty zewnętrzne) poprzez co najmniej zobowiązanie do opracowania procedur. W obecnym stanie wymogi są dość nieprecyzyjne, a w zakresie usługowego prowadzenia ksiąg rachunkowych nie ma wymogu sporządzenia odpowiednich procedur – jedynie czujność, wyobraźnia i zdrowy rozsądek kierownika jednostki motywują do ochrony własnych interesów. Polityka rachunkowości co do zasady może odnosić się do opracowania norm wewnątrz jednostki bez wpływu na zasady obowiązujące w innych jednostkach – biurach rachunkowych. Na gruncie polskim do opracowania takich procedur może posłużyć Krajowy Standard Rachunkowości. Bierne oczekiwanie na zmiany i analiza jedynie wzrastających statystyk ataków w cyberprzestrzeni mogą doprowadzić do generowania niepotrzebnych

kosztów. Trzeba mieć świadomość, że biura obsługi finansowo-księgowej są dobrym celem ataków przestępców w cyberprzestrzeni z uwagi na dostęp do danych większej liczby podmiotów. Pojedynczy atak pozwala na uzyskanie dostępu do danych kilku, kilkudziesięciu lub kilkuset firm. Priorytetem powinno stać się więc zadbanie przez właścicieli biur rachunkowych o właściwe procedury zabezpieczające klientów, co stanowi również zabezpieczenie ich samych. Atak i kradzież danych z cyberprzestrzeni może oznaczać definitywny koniec działalności biura rachunkowego, a co za idzie – wpłynąć na utratę reputacji całej branży usług finansowo-księgowych, zwłaszcza że obecnie przedsiębiorstwa funkcjonują w dobie kryzysu zaufania przy jednoczesnej presji posiadania i przetwarzania danych informatycznych.

Bibliografia

Publikacje

1. Helin A., *Ustawa o rachunkowości. Komentarz*, wyd. 6, C.H. Beck, Warszawa 2014.
2. inFakt, *Księgowy – w biurze czy w chmurze?*, https://www.infakt.pl/front/files/InFakt_-Dzien_Ksiegowego.pdf
3. Klamut E., *Ryzyko w działalności biur rachunkowych*, „Przedsiębiorczość i Zarządzanie", t. XIII, z. 15.
4. Międzynarodowa Federacja Księgowych (IFAC), *Kodeks etyki zawodowych księgowych*, tłum. Stowarzyszenie Księgowych w Polsce, 2011, http://www.skwp.pl/files/zg/Kodeks_etyki_IFAC.pdf
5. Seredyński R., Szaruga K., *Komentarz do ustawy o rachunkowości*, Wydawnictwo ODDK, Gdańsk 2016.
6. Sokołek M., *Zasady odpowiedzialności za rzetelność danych prezentowanych w sprawozdaniu finansowym*, w: *Sprawozdawczość finansowa w systemie wymiany informacji i bezpieczeństwa obrotu gospodarczego*, red. H. Żukowska, M. Zuba-Ciszewska, P. Bolibok, Wydawnictwo KUL, Lublin 2016.
7. *W obronie cyfrowych granic. Czyli 5 rad, aby realnie wzmocnić firmy przed cyber ryzykiem*, PwC, Warszawa, styczeń 2016, www.pwc.pl/badaniebezpieczenstwa
8. *Ustawa o rachunkowości. Komentarz*, red. E. Walińska, wyd. 4, Wolters Kluwer, Warszawa 2016.

Dokumenty prawne

1. Ustawa z dnia 29 września 1994 r. o rachunkowości, DzU z 2016 r., poz. 1047.
2. Komunikat nr 10 Ministra Finansów z dnia 18.05.2010 r. w sprawie ogłoszenia uchwały Komitetu Standardów Rachunkowości w sprawie przyjęcia stanowiska Komitetu w sprawie niektórych zasad prowadzenia ksiąg rachunkowych, Dziennik Urzędowy Ministra Finansów nr 6, poz. 26, http://www.mf.gov.pl/documents/764034/1194473/-DZIENNIK+URZ%C4%98DOWY+MINISTRA+FINANS%C3%93W+NR+6+Z+DNIA+24+CZERWCA+2010+R
3. Załączniki do uchwały nr 1608/38/2010 Krajowej Rady Biegłych Rewidentów z dnia 16 lutego 2010 r.

External Accounting Service and Accounting Policy with regard to Access to Account Books Data

Summary

The period of the last two years has been marked with a rapid technological progress, in particular in the area of tele-information technology. Modern IT solution are used also in business, including accounting. Modern technologies contribute to: cost reduction or easy and fast data processing. Many activities are performed in the cyberspace. However, besides the positive aspects of development of IT technologies, there are visible threats in the form of undesired sharing of accounting data, their deletion or modification. The article deals with the problem of protection of accounting data in the case of corporate accounting service provided by an external entity against the improper access or use. The review has been made of legal acts regulating the question of protection of access to account book data as well as opinions presented by the representative of science. The real threats and methods of protection against accounting cyberattacks have been presented.

Keywords: accounting, data protection, data security, accounting policy, cyberspace, accounting data