STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 47–68

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

Anna Bartoszewicz
Wydział Nauk Ekonomicznych
Uniwersytet Warmińsko-Mazurski w Olsztynie

Proces zarządzania bezpieczeństwem informacji jako element ochrony elektronicznych ksiąg rachunkowych – ujęcie modelowe

Streszczenie

Celem artykułu jest wskazanie roli i etapów procesu zapewnienia bezpieczeństwa informacji w kontekście ochrony elektronicznych danych rachunkowych przetwarzanych w systemach finansowo-księgowych. Cel artykułu został zrealizowany na podstawie interpretacji literatury przedmiotu badań, analizy ustawy o rachunkowości w przedmiotowym zakresie oraz dostępnych na rynku wydawniczym wyników badań empirycznych, prezentowanych przez innych autorów w kontekście tej tematyki. W artykule omówiono wytyczne ustawy o rachunkowości w odniesieniu do ksiąg rachunkowych prowadzonych w systemie FK oraz scharakteryzowano elementy tego systemu. Zamieszczono modelowe rozwiązanie procesu zarządzania bezpieczeństwem informacji w obszarze funkcjonowania systemu FK. Opisano także rolę i etapy audytu bezpieczeństwa informatycznego jako instrumentu zapewniającego prawidłowość jego funkcjonowania. Przeprowadzone rozważania dały podstawę do stwierdzenia, że staranne zaplanowanie i wdrożenie procesu zarządzania bezpieczeństwem informacji w obszarze systemu FK pozwoli na ochronę elektronicznej informacji rachunkowej przed pojawiającymi się zagrożeniami.

Słowa kluczowe: rachunkowość, rachunkowość komputerowa, bezpieczeństwo informacji, audyt bezpieczeństwa informatycznego
Kod klasyfikacji JEL: M410

1. Wprowadzenie

W obecnych czasach zachodzące w szybkim tempie zmiany gospodarcze powodują konieczność pozyskania przez grupy zarządzające informacji ekonomicznej, która jest kluczem do podejmowania decyzji i prawidłowego zarządzania organizacją. Głównym jej źródłem jest rachunkowość, w ramach której są gromadzone i przetwarzane dane dotyczące procesów zachodzących w danym podmiocie, a następnie generuje się z nich informacje, wykorzystywane przez odbiorców wewnętrznych i zewnętrznych jednostki. W XXI w. i dobie technologii informatycznej to jakość i szybkość pozyskanych informacji ma ogromne znaczenie, co w konsekwencji implikuje konieczność zastosowania specjalistycznych narzędzi informatycznych do jej uzyskania. W świetle powyższego, większość jednostek zarówno sektora prywatnego, jak i publicznego prowadzi rachunkowość przy wykorzystaniu komputerowych systemów finansowo-księgowych[1], co z jednej strony znacznie ułatwia generowanie informacji, z drugiej zaś naraża dane rachunkowe na pewne zagrożenia, takie jak ich utrata czy zniekształcenie. W efekcie może to mieć destrukcyjny wpływ na działalność jednostki.

Przeciwdziałając powyższemu, należy przedsięwziąć środki, które pozwoliłyby na zabezpieczenie elektronicznych danych rachunkowych zawartych w systemie finansowo-księgowym przed niepowołanym dostępem lub ich utratą. Rozwiązanie w tej materii może stanowić proces zarządzania bezpieczeństwem informacji, który zaplanowany i prawidłowo wdrożony spełniałby tę funkcję.

Celem niniejszego artykułu jest wskazanie roli i etapów procesu zapewnienia bezpieczeństwa informacji w kontekście ochrony elektronicznych danych rachunkowych przetwarzanych w systemach finansowo-księgowych. Przesłanką do realizacji powyższego celu jest zidentyfikowana przez autorkę artykułu luka badawcza. Analizując bowiem publikacje dostępne na rynku wydawniczym w zakresie procesu zapewnienia bezpieczeństwa informacji w jednostkach, zauważa się, że autorzy

[1] W dalszej części artykułu użyto zamiennie sformułowania „systemy FK".

traktują o tej tematyce w ogólnym zarysie. Dostrzega się natomiast brak odniesienia i modelowych rozwiązań dotyczących bezpieczeństwa elektronicznej informacji rachunkowej. K.J. Knapp i in. wskazują, iż „polityka bezpieczeństwa informacji jest niezbędnym fundamentem programów bezpieczeństwa organizacyjnego, istnieje zatem potrzeba udziału naukowego w tym ważnym obszarze"[2]. Odpowiedzią na powyższe spostrzeżenia jest niniejszy artykuł, który podzielono na dwie części. W pierwszej omówiono wytyczne ustawy o rachunkowości w odniesieniu do ksiąg rachunkowych prowadzonych w systemie FK oraz scharakteryzowano jego elementy. W części drugiej publikacji zamieszczono modelowe rozwiązanie procesu zarządzania bezpieczeństwem informacji w obszarze funkcjonowania systemu FK. Omówiono także rolę i etapy audytu bezpieczeństwa informatycznego jako instrumentu zapewniającego prawidłowość jego działania. Cel artykułu został zrealizowany na podstawie interpretacji literatury przedmiotu badań, analizy ustawy o rachunkowości w przedmiotowym zakresie oraz dostępnych na rynku wydawniczym wyników badań empirycznych, prezentowanych przez innych autorów w kontekście tej tematyki.

2. Wymogi ustawy o rachunkowości w odniesieniu do prowadzenia ksiąg rachunkowych przy użyciu techniki komputerowej

Rachunkowość definiowana jest jako system ewidencyjno-sprawozdawczy, dostarczający informacji ekonomicznej, wykorzystywanej w ocenie działalności przedsiębiorstw i podejmowania decyzji[3]. Innymi słowy, stanowi ona całościowy systemem regularnego gromadzenia i przetwarzania danych, które ostatecznie tworzą informację ekonomiczno-finansową, dotyczącą działalności danego podmiotu.

Rachunkowość jednostki obejmuje[4]:

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

[2] K.J. Knapp, R.F. Morris Jr., T.E. Marshall, T.A. Byrd, *Information security policy: An organizational-level process model*, „Computers & Security" 2009, vol. 28, iss. 7, s. 493.

[3] E. Nowak, *Rachunkowość kurs podstawowy*, PWE, Warszawa 2008, s. 14.

[4] Art. 4 ust. 3 Ustawy z dnia 29 września 1994 r. o rachunkowości, Dz.U. z 2016 r. poz. 1047, 2255 z późn. zm.

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.

Podstawowym aktem prawnym, regulującym zasady prowadzenia rachunkowości, zarówno techniką tradycyjną, jak i z wykorzystaniem systemów informatycznych, jest Ustawa z dnia 29 września 1994 r. o rachunkowości (dalej Uor).

Gdy księgi rachunkowe prowadzone są przy użyciu komputera, za równoważne z nimi uważa się odpowiednio zasoby informacyjne rachunkowości zorganizowane w formie oddzielnych komputerowych zbiorów danych, bazy danych lub wyodrębnionych jej części, bez względu na miejsce ich powstania i przechowywania.

Warunkiem utrzymywania zasobów informacyjnych systemu rachunkowości w formie elektronicznej jest posiadanie przez jednostkę oprogramowania, umożliwiającego uzyskiwanie czytelnych informacji w odniesieniu do zapisów dokonanych w księgach rachunkowych, poprzez ich wydrukowanie lub przeniesienie na informatyczny nośnik danych[5].

Zgodnie z treścią art. 9 Uor, księgi rachunkowe prowadzi się w języku polskim i walucie polskiej, zatem nawet w przypadku korzystania z programu powstałego za granicą musi być on dostosowany do tych wymogów. Ponadto w art. 10 ust. 1 pkt 3 Uor wskazano na konieczność sporządzenia, w przypadku prowadzenia 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. Wymagane jest także sporządzenie 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. Ponadto należy określić wersję oprogramowania i datę rozpoczęcia eksploatacji programu, a także posiadać opis systemu służącego ochronie danych i ich zbiorów, w tym dowodów

[5] Art. 13 Uor.

księgowych, ksiąg rachunkowych i innych dokumentów, stanowiących podstawę dokonanych w nich zapisów.

Wymogi ustawy o rachunkowości w odniesieniu do bezpieczeństwa danych księgowych przetwarzanych za pomocą techniki komputerowej obejmują kilka obszarów. Przede wszystkim „Przy prowadzeniu ksiąg rachunkowych przy użyciu komputera, należy stosować właściwe procedury i środki chroniące przed zniszczeniem, modyfikacją lub ukryciem zapisu"[6]. Zatem w kontekście zachowania bezpieczeństwa informacji rachunkowej należy odpowiedzieć na następujące pytania[7]:

- Czy istnieje procedura odzyskania danych po ewentualnych awariach?
- Czy można ustalić, który pracownik dokonał poszczególnych zapisów księgowych?
- Jakie są zabezpieczenia wprowadzonych zapisów do ksiąg przed ich modyfikacją?

Ochronę danych umożliwia stosowanie odpornych na zagrożenia nośników, dobór stosownych środków ochrony zewnętrznej, systematyczne tworzenie rezerwowych kopii zbiorów danych zapisanych na informatycznych nośnikach danych (pod warunkiem zapewnienia trwałości zapisu informacji systemu rachunkowości), a także zapewnienie ochrony programów komputerowych i danych systemu informatycznego rachunkowości, poprzez stosowanie odpowiednich rozwiązań programowych i organizacyjnych, chroniących przed nieupoważnionym dostępem lub zniszczeniem[8].

Brak możliwości dokonania zapisu w komputerowych księgach rachunkowych po zaksięgowaniu wprowadzonych danych zabezpiecza je przed modyfikacją. Zgodnie z treścią art. 25 ust. 1 Uor, stwierdzony błąd w zapisach poprawia się jedynie przez wprowadzenie do ksiąg rachunkowych dowodu zawierającego korekty dodatnie albo ujemne. Należy podkreślić, że takim zabezpieczeniem nie są objęte dane, które zostały wprowadzone jedynie do bufora[9], nie zaś do ksiąg rachunkowych.

Poprawne zorganizowanie i funkcjonowanie informatycznego systemu rachunkowości leży w gestii kierownika jednostki. Często też podejmuje on decyzję w porozumieniu z głównym księgowym w sprawie zakupu danego programu komputerowego. Ważne jest, aby poza wymogami narzuconymi przez ustawodawcę w odniesieniu do przedmiotowego zakresu rozważyć przy zakupie oprogramowania również kwestię

---

[6] Art. 23 ust. 1 Uor.

[7] Por. T. Cebrowska, *Rachunkowość finansowa*, Wydawnictwo Naukowe PWN, Warszawa 2005, s. 205.

[8] Art. 71 ust. 2 Uor.

[9] Bufor to tzw. brudnopis, który umożliwia sprawdzenie zapisów księgowych przed trwałym ich zaksięgowaniem.

bezpieczeństwa danych rachunkowych, które często narażone są na zniekształcenie lub utratę.

Spełnienie wymogów podanych przez ustawodawcę jest konieczne do prawidłowego prowadzenia ksiąg rachunkowych przy wykorzystaniu systemu FK.

3. Struktura i zastosowanie informatycznego systemu finansowo-księgowego

Jak wskazano wcześniej, rachunkowość jednostki złożona jest z siedmiu elementów, przy czym w kontekście niniejszego opracowania szczególnie ważne jest podkreślenie punktu dotyczącego prowadzenia ksiąg rachunkowych, w których ujmowane są zapisy operacji gospodarczych występujących w jednostce. Ważnym zadaniem rachunkowości jest bowiem ich bieżąca rejestracja, która powinna odbywać się w sposób prawidłowy, kompletny i systematyczny[10]. W tym celu wykorzystuje się określone środki techniczne, za pomocą których rachunkowość prowadzona jest techniką tradycyjną (ręczną) lub jest wspomagana narzędziami komputerowymi.

Obecnie większość firm decyduje się na wybór drugiego rozwiązania z uwagi na oszczędność czasu i szersze zastosowanie. Podkreślenia wymaga fakt, iż informatyzacja rachunkowości wiąże się z koniecznością zakupu programu komputerowego, który będzie wspomagał jej prowadzenie. Wśród dostępnych na rynku ofert w tym zakresie wyróżnia się najczęściej dwa rozwiązania[11]: systemy ewidencyjne oraz zintegrowane systemy ewidencyjno-decyzyjne. Zestawienie porównawcze w ww. zakresie przedstawiono w tabeli 1.

Tabela 1. Zestawienie porównawcze systemów ewidencyjnych oraz zintegrowanych systemów ewidencyjno-decyzyjnych

Wyszczególnienie	Systemy ewidencyjne	Systemy ewidencyjno-decyzyjne
Cel	Ewidencja danych	Zwiększenie efektywności zarządzania
Zbiory danych	Zbiory autonomiczne, niepowiązane	Współpracujące ze sobą podsystemy
Rodzaj danych	Historyczne	Historyczne i planistyczne
Obszar wykorzystania	Rachunkowość finansowa	Rachunkowość zarządcza

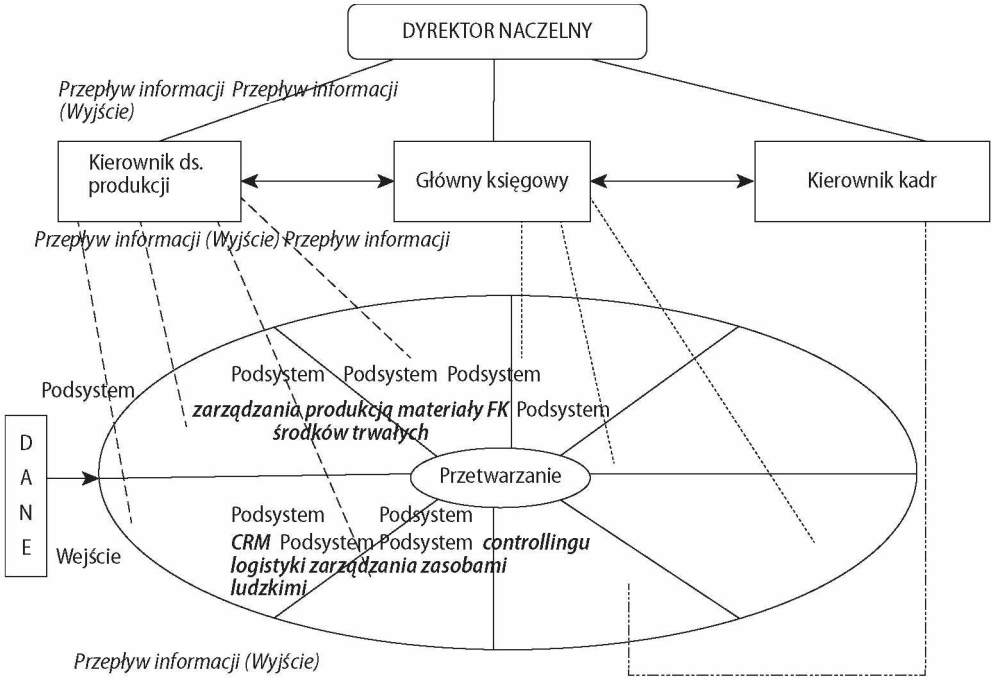
[10] K. Sawicki, *Podstawy rachunkowości*, PWE, Warszawa 2009, s. 15.

[11] Por. Z. Luty, M. Biernacki, A. Kasperowicz, A. Mazur, *Rachunkowość komputerowa*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2010, s. 9.

Wyszczególnienie	Systemy ewidencyjne	Systemy ewidencyjno-decyzyjne
Horyzont czasowy	Działania operacyjne	Działania strategiczne
Operacje standardowe	Rejestrowanie zamówień Pobieranie danych o stanie zapasów Pobieranie i przetwarzanie danych o należnościach i zobowiązaniach Pobieranie danych z kartotek listy płac Rejestrowanie innych danych generowanych w pozostałych podsystemach	Tworzenie raportów o kosztach stałych i zmiennych Wykonywanie budżetów finansowych Projektowanie budżetów finansowych Analiza porównawcza danych rzeczywistych i przewidywanych działań
Przykład systemu	System płac, system finansowo-księgowy, system zarządzania produkcją	Programy dziedzinowe złożone z poszczególnych podsystemów (modułów) – ERP, SAP

Źródło: opracowanie własne na podstawie: W. Wyraz, *Przykłady systemów informacyjnych*, w: *Wstęp do systemów informacyjnych zarządzania w przedsiębiorstwie*, red. A. Nowicki, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2002, s. 240.

Rysunek 1. Struktura zintegrowanego systemu ewidencyjno-decyzyjnego ze wskazaniem kanałów informacyjnych



Źródło: opracowanie własne na podstawie: A. Bytniewski, *Architektura zintegrowanego systemu informatycznego zarządzania*, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław 2005, s. 30.

Należy zauważyć, że w powyższym zestawieniu system finansowo-księgowy został sklasyfikowany jako autonomiczny system ewidencyjny, który służy głównie do rejestracji i przetwarzania danych księgowych. Warto jednak zaznaczyć, że może on również funkcjonować jako jeden z podsystemów zintegrowanego systemu ewidencyjno-decyzyjnego. Przykładową strukturę w tym zakresie zilustrowano na rysunku 1.

Przedstawiona struktura zintegrowanego systemu składa się z ośmiu podsystemów: zarządzania produkcją, materiałów, CRM, logistyki, finansowo-księgowego (FK), środków trwałych, controllingu oraz zarządzania zasobami ludzkimi. W pierwszej kolejności wprowadzane są do systemu „surowe" dane, dotyczące zaistniałych w jednostce zdarzeń, a następnie są one przetwarzane za pomocą systemu informatycznego. Ostatecznym produktem jest ustrukturyzowana informacja, dostarczana kierownictwu w postaci wskaźników, raportów i sprawozdań, dzięki czemu wspierany jest proces decyzyjny w jednostce[12].

Podsystem finansowo-księgowy stanowi rdzeń całego zintegrowanego systemu. Jest on narzędziem wielowymiarowym, bowiem jego zastosowanie pozwala na realizację wielu funkcji[13]. Do najważniejszych należy zaliczyć: funkcję ewidencyjną (gromadzi dane), informacyjną (dostarcza informacji odbiorcom wewnętrznym i zewnętrznym), komunikacyjną (terminowe przekazanie informacji pomiędzy określonymi komórkami w strukturze organizacyjnej jednostki) oraz sprawozdawczą (pozwala na przygotowanie sprawozdań finansowych)[14].

Struktura podsystemu FK złożona jest zwykle z kilku elementów składowych, które w zależności od producenta mogą być różnie nazywane. Przykładowy podział w tym zakresie przedstawiono w tabeli 2.

Decyzja o zinformatyzowaniu rachunkowości zwykle podyktowana jest chęcią usprawnienia pracy w dziele księgowym, stąd przy zakupie programu FK rozpatrywana jest głównie jego funkcjonalność. Patrząc jednak z punktu widzenia bezpieczeństwa danych, które są w nim rejestrowane, agregowane i przetwarzane, należy także zwrócić uwagę na zabezpieczenia systemu przed nieuprawnionym dostępem.

[12] Należy jednak podkreślić, że prezentowany przykład jest jedynie schematycznym rozwiązaniem, dlatego struktura systemu w zależności od przyjętych rozwiązań może być inna.

[13] I. Fabisiak, M. Michnik, *Systemy informatyczne jako narzędzie zarządzania przedsiębiorstwami. Metody analityczne w naukach ekonomicznych – wybrane zastosowania*, red. A. Prędki, Fundacja Uniwersytetu Ekonomicznego w Krakowie, Kraków 2016, s. 157.

[14] A. Chojnacka, B. Niepsujewicz-Misiek, *Podsystem finansowo-księgowy*, w: *Architektura zintegrowanego systemu informatycznego zarządzania*, red. A. Bytniewski, Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu, Wrocław 2005, s. 102.

Prowadzenie bowiem elektronicznych ksiąg rachunkowych narażone jest na liczne zagrożenia. Wszystko to za sprawą cyberprzestępczości, która często skutkuje dostępem osób nieuprawnionych do informacji zawartych w systemach, co w konsekwencji może powodować ich modyfikację lub utratę. Dlatego ważnym aspektem jest odpowiednia ochrona danych w nich zawartych oraz wdrożenie mechanizmów bezpieczeństwa.

Tabela 2. Elementy informatycznego podsystemu finansowo-księgowego

Wyszczególnienie	Charakterystyka i zakres funkcjonowania
Księga główna	Tworzenie planu kont, wprowadzanie wzorca księgowań, dokonywanie przeksięgowań, dekretacja i księgowanie dowodów księgowych, zamykanie roku obrotowego
Moduł „Rozrachunki"	Ewidencja dowodów księgowych związanych z należnościami i zobowiązaniami, głównie faktur VAT sprzedaż/zakup. Z modułu bank pobierane dane o spłacie należności lub zobowiązania
Bank	Ewidencjonowanie wyciągów bankowych (przelewy środków pieniężnych na konto bankowe lub wypłaty z konta bankowego)
Kasa	Ewidencja operacji gospodarczych związanych z przepływem gotówki w jednostce (wpłaty/wypłaty z kasy)
Raporty	Automatyczne tworzenie dziennika operacji księgowych oraz zestawienia obrotów i sald, sporządzanie bilansu oraz rachunku zysków i strat, sporządzanie deklaracji podatkowych, zestawienie należności i zobowiązań, tworzenie innych raportów na potrzeby rachunkowości zarządczej

Źródło: opracowanie własne na podstawie: A. Bytniewski, *Podsystem finansowo-księgowy jako instrument rachunkowości zarządczej i controllingu*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2015, nr 399, s. 114–115.

4. Diagnoza zagrożeń danych zawartych w informatycznych systemach FK oraz proces zarządzania bezpieczeństwem informacji księgowej

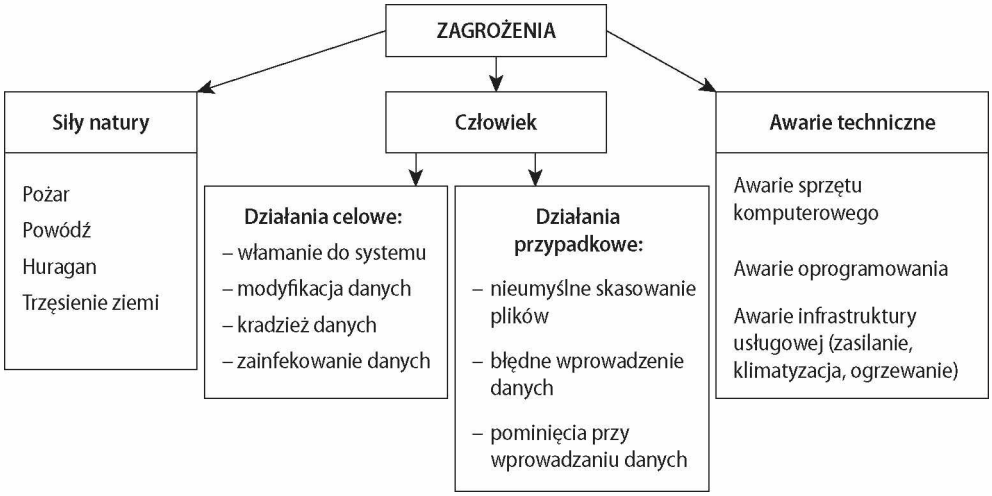
Jak zauważa J. Unold, elementem pierwotnym w stosunku do informacji są „dane", definiowane jako liczby i fakty wyrażone w określonej postaci znakowej, które mogą być przetworzone w informacje przy użyciu sprzętu komputerowego[15].

[15] J. Unold, *Zarządzanie informacją w cyberprzestrzeni*, Wydawnictwo Naukowe PWN, Warszawa 2015, s. 16.

W praktyce gospodarczej występuje szerokie ich spektrum, jednak w kontekście tematyki niniejszego artykułu rozważania odniesiono jedynie do elektronicznych danych rachunkowych, które są odzwierciedleniem operacji gospodarczych, zachodzących w jednostce. W pierwszej kolejności dane wprowadza się do systemu FK z dowodów księgowych (faktur, poleceń księgowania, listy płac itp.), a następnie są one przetwarzane w informację, która zawarta w sprawozdaniach finansowych stanowi główne źródło wiedzy dla szerokiego grona odbiorców.

W toku działalności gospodarczej elektroniczne dane rachunkowe narażone są na różnego rodzaju zagrożenia, określane jako potencjalne przyczyny wystąpienia niekorzystnego zjawiska, które może spowodować szkody dla systemu lub organizacji i jej aktywów[16]. Przykładowy podział zagrożeń w odniesieniu do elektronicznych danych księgowych przedstawiono na rysunku 2.

Rysunku 2. Podział zagrożeń elektronicznych danych księgowych



Źródło: opracowanie własne na podstawie: K. Lidernan, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 155.

Badania ankietowe przeprowadzone przez M. Pałęga i in. potwierdzają tezę, że najsłabszym ogniwem w systemie bezpieczeństwa informacji jest czynnik ludzki. W większości przypadków ankietowani wskazywali na wewnętrzne bądź zewnętrzne

[16] M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Wydawnictwo Helion, Gliwice 2007, s. 79.

źródła zagrożeń, które wiążą się z różnorodną aktywnością człowieka. Wśród typowych zachowań personelu determinujących wyciek informacji z firmy wskazano: „łamanie obowiązujących procedur, niefrasobliwość oraz lekkomyślność, nadmierne zaufanie do osób trzecich, a także nadmierne gadulstwo. [...] Najistotniejszym źródłem wycieku informacji okazała się również podatność na wpływ osób trzecich"[17]. Zagrożenie może mieć zarówno pochodzenie wewnętrzne, w przypadku działania pracownika na szkodę jednostki, jak i zewnętrzne, kiedy dochodzi do szpiegostwa dokonanego przez konkurencję. Ponadto wystąpienie określonych zagrożeń uwarunkowane jest takimi czynnikami, jak: środowisko, branża czy też kultura organizacyjna jednostki. Z uwagi na tak szeroki zakres zagrożeń istnieje konieczność wdrożenia odpowiednich zabezpieczeń, które pozwolą na ochronę elektronicznych danych rachunkowych, a tym samym zabezpieczą informację generowaną przez system FK.

Jednym z rozwiązań jest opracowanie i wdrożenie procesu zarządzania bezpieczeństwem informacji w obszarze elektronicznych ksiąg rachunkowych[18]. Bezpieczeństwo w potocznym znaczeniu jest rozumiane jako stan niezagrożenia i od wieków jest pożądane w wielu sferach aktywności człowieka[19]. W odniesieniu do bezpieczeństwa informacji jest ono związane z niezakłóconym funkcjonowaniem procesów w organizacji[20], stąd ważne jest, aby informacja w danym podmiocie była odpowiednio chroniona. Szczególne bezpieczeństwo należy zapewnić informacji rachunkowej, którą uznaje się za bardzo ważny rodzaj aktywa zarówno w jednostkach sektora publicznego, jak i prywatnego. Pomocne w tej materii będzie wdrożenie w organizacji procesu zarządzania bezpieczeństwem informacji.

Powyższy proces należy zdefiniować jako przebieg następujących po sobie powiązanych przyczynowo etapów, które pozwalają na zabezpieczenie informacji

[17] M. Pałęga, M. Knapiński, W. Kulma, *Ocena systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie w świetle przeprowadzonych badań*, Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją (PTZP), Opole 2014, s. 428–429.

[18] Podkreślenia wymaga to, że proces zarządzania bezpieczeństwem informacji w obszarze funkcjonowania systemu FK jest jedynie wybraną częścią odnoszącą się tylko do sfery rachunkowo-finansowej jednostki. Należy jednak zwrócić uwagę, iż organizacja powinna wdrożyć proces zarządzania bezpieczeństwem informacji do wszystkich obszarów w podmiocie, w celu ochrony danych elektronicznych. Standardy w tym zakresie określone zostały przez Polski Komitet Normalizacyjny w normie PN-ISO/ISC 27001:2014–12. Ponadto regulacje w tym obszarze dla jednostek sektora finansów publicznych wskazane są w Rozporządzeniu Rady Ministrów z 2012 r. w sprawie Krajowych Ram Interoperacyjności.

[19] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa, 2007, s. 27.

[20] J. Łuczak, *Ochrona danych osobowych jako element zarządzania bezpieczeństwem informacji*, „Studia Oeconomica Posnaniensja" 2016, vol. 4, no. 12, s. 59.

rachunkowej przed jej zniekształceniem lub utratą. Punktem wyjścia do tego procesu jest bezpieczeństwo systemów informatycznych, bowiem informacja rachunkowa generowana jest z danych, które przetwarzane są w większości podmiotów z wykorzystaniem powyższych systemów. Analizując publikacje różnych autorów, zauważa się, że podają oni różną liczbę etapów przebiegu samego procesu zarządzania bezpieczeństwem systemów informatycznych. Przykładowo Stawowski[21] wyróżnia tylko kilka głównych etapów, natomiast Piotrowski i Szymaczek[22] czy Rzewulski[23] podają ich znacznie więcej, rozwijając ten proces. Tak różny poziom szczegółowości w przedstawieniu procesu zarządzania bezpieczeństwem systemu informatycznego jest często uzasadniony i wynika z faktu, że istnieją różne sposoby zarządzania, a także różne rozmiary i struktura podmiotów. Zatem proces ten musi zostać dopasowany do środowiska, w którym będzie realizowany. Istotne jest, aby wszystkie jego etapy odpowiadały stylowi, wielkości, strukturze i sposobowi prowadzenia działalności danej jednostki[24]. Modelowy proces zarządzania bezpieczeństwem informacji w systemie FK mógłby przebiegać w trzech fazach: projektowania, wdrożenia oraz monitorowania, obejmując łącznie osiem kolejnych etapów. Szczegółowy podział w tym zakresie zaprezentowano na rysunku 3.

Zgodnie z przedstawionym schematem, w fazie pierwszej (zaprojektowanie) dochodzi do opracowania dokumentu zwanego polityką bezpieczeństwa informacji, która stanowi zbiór określonych zasad i reguł, opisujących sposób przetwarzania, zarządzania i przechowywania danych w systemach finansowo-księgowych. W dokumencie tym zaleca się zawrzeć m.in. następujące elementy[25]:

- ogólne cele, zakres oraz znaczenie bezpieczeństwa jako mechanizmu,
- wyjaśnienie zasad, norm i wymagań polityki (np. wymagania odnośnie do szkoleń w zakresie bezpieczeństwa, konsekwencje w przypadku naruszenia polityki),
- ogólne kompetencje i obowiązki pracowników w odniesieniu do zarządzania bezpieczeństwem informacji systemów FK,
- podział obowiązków poszczególnych osób w zakresie realizacji polityki bezpieczeństwa.

---

[21] M. Stawowski, *Ochrona informacji w sieciach komputerowych*, Wydawnictwo ArsKom, Warszawa 1998.

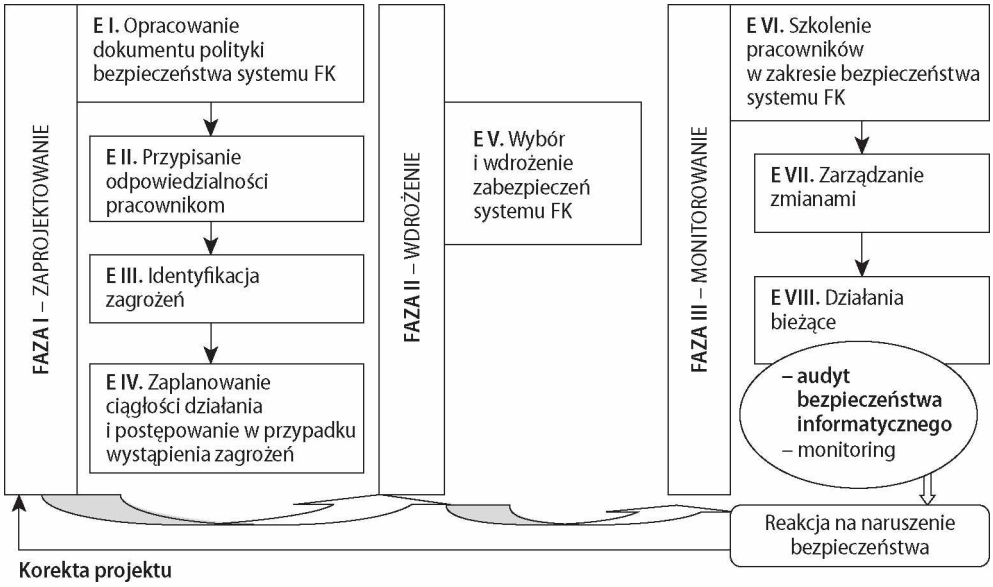
[22] J. Piotrowski, M. Szymaczek, *Projektowanie skutecznych systemów ochrony informacji*, „Informatyka" 1997, nr 7–8.

[23] M. Rzewulski, *Jak przetrwać katastrofę?*, „PC Kurier" 2002, nr 3.

[24] J. Madej, J. Sztorc, *Proces zarządzania bezpieczeństwem systemu informatycznego w przedsiębiorstwie*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, nr 798, s. 246.

[25] Polska Norma PN-ISO/ISC 27001:2014–12.

Rysunek 3. Proces zarządzania bezpieczeństwem informacji w obszarze funkcjonowania systemu FK



Źródło: opracowanie własne.

Ważnym elementem na tym etapie jest również wskazanie administratora bezpieczeństwa informacji (ABI), którego rolą jest koordynacja całego procesu. W opracowanie dokumentu zaangażowani są także informatycy, główny księgowy oraz kierownik jednostki. Polityka bezpieczeństwa informacji powinna być znana i zrozumiana przez wszystkich pracowników firmy.

W kolejnym etapie następuje nadanie uprawnień użytkownikom (są to zwykle pracownicy działu księgowości) do pracy w systemie FK poprzez przypisanie loginu. Konieczne jest także utworzenie haseł, których weryfikacja pozwoli na uwierzytelnienie użytkowników.

Etap trzeci polega na identyfikacji zagrożeń dla danych księgowych, które są przetwarzane w systemie FK oraz informacji generowanych przez ten system. Lista i podział zagrożeń zostały już wcześniej podane, należy jednak podkreślić, że nie jest to katalog zamknięty, bowiem w zależności od uwarunkowań otoczenia, w jakim funkcjonuje dana jednostka, mogą pojawić się inne rodzaje niebezpieczeństw.

Fazę pierwszą zamyka etap planowania ciągłości działania i postępowania w przypadku wystąpienia zagrożeń, który opiera się na opracowaniu i wdrożeniu

planów odtworzenia zapisów księgowych, zapewniających dostępność informacji na wymaganym poziomie i w wymaganym czasie w przypadku wystąpienia awarii systemu FK[26].

Zaprojektowanie procesu zarządzania bezpieczeństwem informacji pozwala przejść do realizacji fazy wdrożenia, która polega na wyborze i implementacji zabezpieczeń systemu FK. Są one określane jako pewne mechanizmy, umożliwiające zredukowanie stopnia wystąpienia ryzyka awarii systemu lub modyfikacji/kradzieży danych w nim zawartych. Przykładowe zabezpieczenia w odniesieniu do bezpieczeństwa informacji w systemach FK są następujące:

- dodatkowe zasilanie serwera,
- mechanizmy kontroli dostępu (loginy, hasła itp.),
- autoryzacja,
- oprogramowanie antywirusowe,
- ochrona przed kodem złośliwym i kodem mobilnym,
- zabezpieczenie fizyczne (zamki, ochrona, kamery monitoringu itp.),
- kopie bezpieczeństwa.

Jak wskazują wyniki badań przeprowadzone przez R. Walaska w 2014 r.[27], najczęściej stosowane zabezpieczenia danych w przedsiębiorstwach logistycznych są następujące: oprogramowania antywirusowe (91% badanych firm), kopie zapasowe 70% ankietowanych, mechanizmy kontroli dostępu 57%, zasilanie rezerwowe 53% badanych jednostek. Oprogramowanie antywirusowe stanowi obecnie podstawę systemu bezpieczeństwa informacyjnego każdego przedsiębiorstwa. Dzieje się tak dlatego, że statystycznie największym zagrożeniem dla bezpieczeństwa danych są ataki hakerskie z sieci Internet w postaci różnego rodzaju wirusów, które po zainstalowaniu na komputerze zaczynają potajemnie przesyłać informacje z jego dysków. Nowoczesne oprogramowanie antywirusowe pozwala natomiast na skuteczną eliminację tych zagrożeń poprzez kontrolowanie wszystkich plików przychodzących i wyłapywanie tych, które są podejrzane i stanowią potencjalne niebezpieczeństwo. Nowoczesne programy antywirusowe identyfikują i aktualizują również nowo pojawiające się zagrożenia[28].

---

[26] Por. ibidem.

[27] Badanie ankietowe zostało przeprowadzone w 2014 r. przez R. Walaska na próbie 93 firm logistycznych województwa łódzkiego. Celem była próba określenia poziomu wdrożenia i wykorzystania systemów bezpieczeństwa informacji w wybranych obszarach działalności logistycznej.

[28] R. Walasek, *Systemy bezpieczeństwa informacji w przedsiębiorstwach logistycznych – wyniki badania*, „Nauki o Zarządzaniu. Management Sciences" 2016, 1(26), Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, s. 161.

Trzecia faza procesu polega na upowszechnianiu przyjętych rozwiązań i monitorowaniu prawidłowości ich przebiegu. Należy ją rozpocząć przeszkoleniem pracowników działu księgowego w zakresie bezpieczeństwa systemu FK. Kolejnym etapem jest zarządzanie zmianami i opiera się na identyfikacji nowych wymagań w zakresie bezpieczeństwa, do jakich trzeba przystosować system FK w przypadku aplikacji jakichkolwiek zmian. Mogą one przykładowo dotyczyć nowych procedur i funkcji systemu, zmian sprzętowych, aktualizacji oprogramowania, pojawienia się nowych użytkowników czy też wprowadzenia dodatkowych połączeń sieciowych[29].

Nieodzownym elementem ostatniej fazy procesu zarządzania bezpieczeństwem informacji jest monitoring bezpieczeństwa danych i informacji generowanych przez system FK, podczas którego identyfikuje się wszelkie przypadki kwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczeń systemu FK. Należą do nich m.in.:

- nieprzewidziane działanie sił natury, tj. powódź, pożar czy huragan,
- awarie sprzętu komputerowego, wskazujące na umyślne działanie w kierunku modyfikacji danych w systemie FK,
- pojawienie się komunikatu alarmowego wskazującego na zagrożenie utraty danych,
- odstępstwo od stanu pożądanego, wskazujące na modyfikację danych,
- stwierdzona próba dostępu do systemu bez nadanego uprawnienia (autoryzacji).

Z przeprowadzonych badań wynika, iż obszarem najczęściej monitorowanym przez nowoczesne narzędzia jest obszar sieci (Internet), tak wskazało 70% ankietowanych, oraz systemy operacyjne (prawie połowa ankietowanych zaznaczyła tę odpowiedź). Ponadto wraz ze wzrastającą świadomością dotyczącą ochrony danych prawie połowa badanych przedsiębiorstw coraz częściej decydowała się na monitorowanie własnego personelu. Ponadto monitorowano takie obszary, jak: system bazy danych (38% ankietowanych wskazało tę odpowiedź), aplikacje (37%) oraz sprzęt (35%)[30].

Poza cyklicznym szkoleniem pracowników działu księgowego w przedmiotowym zakresie oraz prowadzeniem bieżących działań monitoringowych, weryfikację prawidłowości funkcjonowania procesu bezpieczeństwa informacji systemów FK należy poddać specjalistycznemu audytowi. Jego przeprowadzenie jest podstawą wydania zapewnienia dla kierownika jednostki na temat właściwego przebiegu procesu zarządzania bezpieczeństwem informacji w obszarze funkcjonowania systemu FK.

[29] J. Unold, *Zarządzanie...*, op.cit., s. 89.

[30] R. Walasek, *Systemy...*, op.cit., s. 162.

5. Audyt bezpieczeństwa informatycznego w obszarze systemu FK

Audyt bezpieczeństwa informatycznego jest zagadnieniem obszernym, a tym samym trudnym do jednoznacznego zdefiniowania. Punktem wyjścia do interpretacji tego pojęcia jest audyt informatyczny, który obejmuje zasoby wchodzące w skład środowiska informatycznego. Do najważniejszych zalicza się weryfikację stanu bezpieczeństwa systemów informatycznych oraz w razie potrzeby pojedynczych aplikacji z perspektywy występującego ryzyka oraz zaimplementowanych procedur kontrolnych. Zatem audyt bezpieczeństwa systemów informatycznych stanowi jego składową[31].

W odniesieniu do systemu FK audyt bezpieczeństwa informatycznego obejmuje przede wszystkim identyfikację zagrożeń dla systemu FK oraz weryfikację jego zabezpieczeń. Podjęcie czynności audytowych ma na celu wspieranie optymalizacji procesu zarządzania bezpieczeństwem informacji generowanej przez system FK, podniesienie bezpieczeństwa księgowanych danych oraz minimalizację ryzyka związanego z wystąpieniem określonych zagrożeń.

Audyt bezpieczeństwa informatycznego w obszarze FK powinien obejmować pięć etapów[32]:

- Etap I. Wskazanie obszarów przewidzianych do audytu
- Etap II. Identyfikacja ryzyka zagrażającego prawidłowemu funkcjonowaniu systemu FK
- Etap III. Określenie kryteriów i wag dla poszczególnych obszarów
- Etap IV. Przeprowadzenie testów
- Etap V. Przygotowanie sprawozdania z audytu i wydanie zaleceń.

W ramach pierwszego etapu audytor wskazuje newralgiczne punkty systemu FK, które narażone są na wystąpienie określonych rodzajów ryzyka. Są to obszary, które zostaną poddane ocenie w toku przeprowadzania audytu bezpieczeństwa informatycznego. Zakres ten może obejmować przykładowo:

[31] S. Bartoszewicz, A. Bartoszewicz, *Rola i zadania audytu bezpieczeństwa systemów informatycznych na przykładzie jednostki sektora administracji rządowej*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, Finanse, Rynki Finansowe, Ubezpieczenia" 2016, nr 6(80), część 1, Uniwersytet Szczeciński, s. 270–271.

[32] Wskazany przykład jest ujęciem modelowym. W zależności od struktury organizacyjno-prawnej jednostki, liczba i nazwa etapów może być różna.

- Obszar 1 – Bezpieczeństwo fizyczne i środowiskowe,
- Obszar 2 – Kontrolę dostępu do systemu FK,
- Obszar 3 – Zarządzanie ciągłością działania systemu FK,
- Obszar 4 – Zarządzanie systemem FK.

Po ich wyznaczeniu do każdego obszaru przypisuje się ryzyko, które może pojawić się w toku działalności podmiotu i zagrażać rzetelności informacji zawartej w elektronicznych księgach rachunkowych, prowadzonych w jednostce przy wykorzystaniu systemu finansowo-księgowego. W tabeli 3 zamieszczono wybrane rodzaje ryzyka w ramach obszarów zidentyfikowanych na pierwszym etapie audytu.

Tabela 3. Wybrane rodzaje ryzyka w ramach obszarów przewidzianych do audytu bezpieczeństwa informatycznego

Obszar	Przykład ryzyka
Bezpieczeństwo fizyczne i środowiskowe	• Nieodpowiednie fizyczne bariery chroniące przed nieuprawnionym dostępem (np. blokada wejścia do budynku) • Nieodpowiednie zabezpieczenia alarmowe miejsc, w których zlokalizowane są kluczowe jednostki systemu, tj. komputery, serwer (alarm przeciwpożarowy, alarm przeciwpowodziowy) • Nieodpowiednia fizyczna kontrola dostępu do obszarów, gdzie są przetwarzane oraz przechowywane dane księgowe (np. monitoring pomieszczeń lub wejść do budynku)
Kontrola dostępu do systemu FK	• Dostęp do systemu FK osób nieuprawnionych • Niewłaściwe przydzielenie praw dostępu dla użytkowników systemu • Brak odpowiedniej autoryzacji wniosku o przyznanie dostępu • Brak dokumentów potwierdzających zrozumienie warunków dostępu przez użytkowników • Niezapewnienie odpowiednich haseł do weryfikacji tożsamości użytkownika systemu
Zarządzanie ciągłością działania systemu FK	• Nieokreślenie wszystkich aktywów zaangażowanych w krytyczne procesy • Nieposiadanie odpowiednich ubezpieczeń na wypadek przerwania ciągłości działania • Nieprzeprowadzenie testów i aktualizacji • Nieposiadanie planów awaryjnych
Zarządzanie systemem FK	• Brak kopii zapasowych • Niezidentyfikowanie i niezarejestrowanie zmian w systemie • Nieuprawnione lub nieumyślne modyfikacje lub niewłaściwe użycie systemu

Źródło: opracowanie własne na podstawie Polskiej Normy PN-ISO/ISC 27001:2014–12.

W trzecim etapie audytu następuje przypisanie kryteriów i wag poszczególnym obszarom audytu, które wskazano w etapie pierwszym. Wagi te przyznawane są subiektywnie przez audytora i obrazują poziom ryzyka oraz ważność danego

obszaru; ich suma musi wynosić 100 pkt. Przykładowy rozkład wag może być następujący: Obszar 1 – Bezpieczeństwo fizyczne i środowiskowe **20 pkt.**; Obszar 2 – Kontrola dostępu do systemu FK **30 pkt.**; Obszar 3 – Zarządzanie ciągłością działania systemu FK **30 pkt.**; Obszar 4 – Zarządzanie systemem FK **20 pkt.**

Czwarty etap audytu polega na przeprowadzeniu testów, które są narzędziem weryfikacji poprawności funkcjonowania i zabezpieczeń systemu FK. Są one zwykle przeprowadzane z wykorzystaniem listy kontrolnej, która pozwala na dokonanie analizy prawidłowości funkcjonowania systemu pod kątem procesów zachodzących w jednostce. Ponadto można wykorzystać także testowanie zabezpieczeń i danych systemu FK.

Etapem kończącym audyt jest sporządzenie sprawozdania, w którym audytor wskazuje ustalenia i wydaje zalecenia, które w jego opinii należy wdrożyć w celu usprawnienia funkcjonowania systemu finansowo-księgowego. Przykładowe ustalenia zamieszczono poniżej.

A. W zakresie kontroli dostępu do systemu:
   - brak procedury zatwierdzania dostępu do systemu (nie wskazano osoby zatwierdzającej dostęp i podstawy, na mocy której działa);
   - brak weryfikacji zakresu nadanych uprawnień z faktycznym dostępem do zasobów i usług sieciowych (nie wskazano osoby odpowiedzialnej);
   - konto użytkownika do systemu nie jest blokowane po wpisaniu błędnego hasła.

B. W zakresie bezpieczeństwa fizycznego i środowiskowego:
   - brak weryfikacji skuteczności zastosowanych zabezpieczeń fizycznych oraz brak wskazania osoby odpowiedzialnej w tym zakresie,
   - kopie zapasowe nie są regularnie sprawdzane i testowane, a także brak jest osoby odpowiedzialnej za te czynności,
   - procedury odtwarzania nie są regularnie sprawdzane i testowane, a także brak jest osoby odpowiedzialnej za te czynności.

Przeprowadzenie audytu bezpieczeństwa informatycznego w obszarze systemu FK ma na celu zapewnienie obiektywnej i niezależnej oceny jego funkcjonowania. Ponadto potwierdzona zostaje skuteczność oraz bezpieczeństwo wdrożonych w jednostce mechanizmów kontrolnych w tym zakresie.

6. Podsumowanie

Reasumując powyższe rozważania, należy podkreślić, że badania przeprowadzone przez organizację ISO w 2015 r. wskazują, iż certyfikat zgodności systemów zarządzania bezpieczeństwem informacji z normą PN-ISO/IEC 27001 uzyskało w Polsce 448 organizacji. Stanowi to znaczny przyrost w stosunku do roku poprzedniego, gdzie takich podmiotów było 310. Również na całym świecie odnotowano blisko 20-procentowy wzrost organizacji, które uzyskały ten certyfikat. Do 10 krajów posiadających najwięcej certyfikatów ISO/IEC 27001 w 2015 r. zaliczono: Japonię – 8240; Zjednoczone Królestwo – 2790; Indie – 2490 oraz Chiny – 2469[33].

Niepokojący jest natomiast fakt, iż audyt dotyczący zgodności z normą PN-ISO/IEC 27001 wykonało zaledwie 24 urzędów[34] w Polsce, mimo że wymogi powyższego działania wymienione zostały w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Należy podkreślić, iż informacja rachunkowa jest uważana za rodzaj aktywa niezbędnego do prowadzenia działalności biznesowej organizacji, dlatego jednym z priorytetów dla kierownictwa jednostek zarówno sektora publicznego, jak i prywatnego powinna być jej ochrona. Jest to szczególnie ważne w przypadku informacji generowanej przez system FK, w którym są przetwarzane dane księgowe. W wyniku dostępu do sieci szerokiego grona użytkowników informacja ta jest narażona na stale zwiększającą się liczbę zagrożeń, co może powodować zainfekowanie danych, jak również ich utratę. W efekcie końcowym naraża to jednostkę na koszty pomocy technicznej i serwisu, a także rośnie ryzyko nieterminowej realizacji zobowiązań.

Rozwiązaniem tego problemu jest staranne zaplanowanie i wdrożenie procesu zarządzania bezpieczeństwem informacji w obszarze systemu FK, który pozwoli na wsparcie realizacji etapów księgowych w danym podmiocie, a także ochroni

[33] Por. ISO Survey 2015, *Executed Summary*, International Standards Organization.

[34] Wyniki badania przeprowadzonego przez Izbę Rzeczoznawców Polskiego Towarzystwa Informatycznego na próbie ok. 340 samorządów pt. „Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego" wskazują, że „Zdecydowana większość instytucji, tj. 309, co stanowi ponad 91% badanych, nie zakupiła ani jednej normy" (w badaniu IR PTI pytała o PN-ISO/IEC 20000 PN-ISO/IEC 27001 PN-ISO/IEC 27005 PN-ISO/IEC 24762).

informację przed zniekształceniem. Pomocne w tej materii będzie także przeprowadzenie audytu bezpieczeństwa informatycznego, który da podstawy wydania obiektywnego zapewnienia o prawidłowym funkcjonowaniu systemu.

Bibliografia

Dokumenty prawne

1. Polski Komitet Normalizacyjny, Polska Norma PN-ISO/ISC 27001:2014–12. *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, Warszawa 2014.
2. Rozporządzenie Rady Ministrów z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. z 2012 r., poz. 526.
3. Ustawa z dnia 29 września 1994 r. o rachunkowości, Dz.U. z 2016 r., poz. 1047, 2255 z późn. zm.

Wydawnictwa zwarte

1. Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2007.
2. Bytniewski A., *Architektura zintegrowanego systemu informatycznego zarządzania*, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław 2005.
3. Cebrowska T., *Rachunkowość finansowa*, Wydawnictwo Naukowe PWN, Warszawa 2005.
4. Chojnacka A., Niepsujewicz-Misiek B., *Podsystem finansowo-księgowy*, w: *Architektura zintegrowanego systemu informatycznego zarządzania*, red. A. Bytniewski, Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu, Wrocław 2005.
5. Fabisiak I., Michnik M., *Systemy informatyczne jako narzędzie zarządzania przedsiębiorstwami. Metody analityczne w naukach ekonomicznych – wybrane zastosowania*, red. A. Prędki, Fundacja Uniwersytetu Ekonomicznego w Krakowie, Kraków 2016.
6. *Komentarz do ustawy o rachunkowości*, red. A. Jarugowa, T. Martyniuk, ODDK, Gdańsk 2009.
7. Lidernan K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.

8. Luty Z., Biernacki M., Kasperowicz A., Mazur A., *Rachunkowość komputerowa*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2010.
9. Molski M., Łacheta M., *Przewodnik audytora systemów informatycznych*, Wydawnictwo Helion, Gliwice 2007.
10. Nowak E., *Rachunkowość kurs podstawowy*, PWE, Warszawa 2008.
11. *Rachunkowość finansowa*, red. R. Cebrowska, Wydawnictwo Naukowe PWN, Warszawa 2005.
12. Sawicki K., *Podstawy rachunkowości*, PWE, Warszawa 2009.
13. Stawowski M., *Ochrona informacji w sieciach komputerowych*, Wydawnictwo ArsKom, Warszawa 1998.
14. Unold J., *Zarządzanie informacją w cyberprzestrzeni*, Wydawnictwo Naukowe PWN, Warszawa 2015.
15. Wyraz W., *Przykłady systemów informacyjnych*, w: *Wstęp do systemów informacyjnych zarządzania w przedsiębiorstwie*, red. A. Nowicki, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2002.

Artykuły prasowe i okolicznościowe

1. Bartoszewicz S., Bartoszewicz A., *Rola i zadania audytu bezpieczeństwa systemów informatycznych na przykładzie jednostki sektora administracji rządowej*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego Finanse, Rynki Finansowe, Ubezpieczenia" 2016, nr 6(80), cz. 1, Uniwersytet Szczeciński.
2. Bytniewski A., *Podsystem finansowo-księgowy jako instrument rachunkowości zarządczej i controllingu*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2015, nr 399.
3. Łuczak J., *Ochrona danych osobowych jako element zarządzania bezpieczeństwem informacji*, „Studia Oeconomica Posnaniensja", 2016, vol. 4, no. 12.
4. ISO Survey 2015, *Executed Summary*, International Standards Organization.
5. Knapp K.J., Morris Jr. R.F., Marshall T.E., Byrd T.A., *Information Security Policy: An Organizational-Level Process Model*, „Computers & Security" 2009, vol. 28, iss. 7.
6. Madej J., Sztorc J., *Proces zarządzania bezpieczeństwem systemu informatycznego w przedsiębiorstwie*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, nr 798.
7. Pałęga M., Knapiński M., Kulma W., *Ocena systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie w świetle przeprowadzonych badań*, Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją (PTZP), Opole 2014, s. 419–428.
8. Piotrowski J., Szymaczek M., *Projektowanie skutecznych systemów ochrony informacji*, „Informatyka" 1997, nr 7–8.

9. Rzewulski M., *Jak przetrwać katastrofę?*, „PC Kurier" 2002, nr 3.
10. Walasek R., *Systemy bezpieczeństwa informacji w przedsiębiorstwach logistycznych – wyniki badania*, „Nauki o Zarządzaniu. Management Siences" 2016, 1(26), Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Information Security Process Management as an Element of Electronic Account Books Protection. Model Approach

Summary

The aim of this article is to indicate the role and stages of the information security process in the context of electronic accounting data protection processed in the financial accounting systems. The aim was achieved on the basis of the literature interpretation, analysis of the Law on accounting within the topical scope as well as results of empirical research on the subject published by other authors. The article discusses the guidelines of the Law on accounting with regard to account books in the financial accounting system and describes the elements of the system. It includes a model solution to the process of information security management in the area of the financial-accounting system. It also describes the role and stages of IT security audits as an instrument to guarantee its correct functioning. The conducted study gave rise to the statement that a careful planning and implementation of the information security management process in the area of the financial-accounting system will allow for the protection of electronic accounting information against emerging threats.

Keywords: accounting, computer accounting, information security, IT security audit