STUDIA I PRACE

Kolegium Zarządzania i Finansów

ZESZYT NAUKOWY 157

STUDIA I PRACE

Kolegium Zarządzania i Finansów

ZESZYT NAUKOWY 157

SGH

SZKOŁA GŁÓWNA HANDLOWA W WARSZAWIE

Tłumaczenie streszczeń artykułów do czasopisma „Studia i Prace KZiF" – zadanie finansowane w ramach umowy 767/P-DUN/2017 ze środków Ministra Nauki i Szkolnictwa Wyższego przeznaczonych na działalność upowszechniającą naukę.

Czasopismo ukazuje się w wersji papierowej (jest to wersja pierwotna) i elektronicznej

ISSN 1234-8872

Nakład 250 egz.

Oficyna Wydawnicza SGH – Szkoła Główna Handlowa w Warszawie
02-554 Warszawa, al. Niepodległości 162
www.wydawnictwo.sgh.waw.pl, e-mail: wydawnictwo@sgh.waw.pl

Projekt okładki
Małgorzata Przestrzelska

Aktualizacja okładki
ADYTON

Skład i łamanie
DM Quadro

Druk i oprawa
QUICK-DRUK s.c.

Zamówienie 166/X/17

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 5–6

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

Spis treści

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 7–8

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

Od Rady Naukowej

Przekazujemy w Państwa ręce 157. numer zeszytu „Studia i Prace Kolegium Zarządzania i Finansów". Artykuły w nim zamieszczone dotyczą aktualnych zagadnień ekonomii, finansów i nauk o zarządzaniu. W bieżącym numerze wiele uwagi zostało poświęcone zagadnieniom związanym z wpływem cyfryzacji na rachunkowość. W poszczególnych artykułach zaprezentowano wyniki najnowszych badań oraz zdiagnozowano stojące przed naukowcami wyzwania związane z cyberprzestrzenią i systemami informacji finansowej. Wyrażamy nadzieję, że wiedza zawarta w tym zeszycie stanowić będzie istotny wkład w rozwój polskiej nauki o finansach i zarządzaniu.

W pierwszym artykule Elżbieta Izabela Szczepankiewicz omówiła zagrożenia dla zasobów informatycznych rachunkowości, które w dobie transformacji *Information Technology* występują w jednostkach sektora finansów publicznych.

Celem drugiego artykułu, autorstwa Grażyny Voss, było pokazanie zmian wynikających z wdrożenia procesu cyfryzacji w rachunkowości oraz korzyści i zagrożeń wynikających z tego procesu.

W następnym artykule Anna Bartoszewicz zaprezentowała, w ujęciu modelowym, proces zarządzania bezpieczeństwem informacji jako element ochrony elektronicznych ksiąg rachunkowych.

W kolejnym artykule Jolanta Wiśniewska przedstawiła uregulowania prawne oraz zagrożenia dla rachunkowości, wynikające z rozwoju nowych technologii, metody ich wykrywania i zapobiegania im.

Problemem cyberprzestępczości i związanych z nią kosztów zajęła się w swoim artykule Beata Dratwińska-Kania. Autorka omówiła zagadnienie z perspektywy rachunkowości.

Magdalena Kludacz-Alessandri w swoim artykule podjęła próbę analizy stopnia komputeryzacji szpitali i oceny wpływu tego czynnika na jakość rozwiązań w zakresie kalkulacji kosztów procesu leczenia pacjenta oraz stopień wykorzystania informacji kosztowych w procesie zarządzania szpitalem.

Celem artykułu Beaty Sadowskiej było znalezienie odpowiedzi na pytanie: Czy System Informatyczny Lasów Państwowych pozwala na generowanie i prezentowanie kompleksowej informacji o ich działalności?

W następnym artykule autorzy Jarosław Bogusław Wedler i Piotr Szczypa przedstawili czasoprzestrzeń rachunkową kont wielostronnych jako podstawę oprogramowania finansowo-księgowego.

Udzielenie odpowiedzi na pytanie o rolę, jaką odgrywają analitycy giełdowi na polskim rynku kapitałowym wobec kształtowania wyniku finansowego przez zarządy spółek notowanych na Giełdzie Papierów Wartościowych w Warszawie, stanowiło cel artykułu Piotra Wójtowicza.

W ostatnim artykule Michał Comporek zajął się ilościową i wartościową analizą sankcji cywilnoprawnych nakładanych przez KNF na emitentów papierów wartościowych oraz podmioty z nimi powiązane w związku z niewypełnianiem lub nierzetelnym wypełnianiem obowiązku informacyjnego.

Mamy nadzieję, że prezentowane artykuły spotkają się z Państwa życzliwym zainteresowaniem oraz, co byłoby szczególnie cenne, staną się przyczynkiem do polemiki i dalszych owocnych badań.

Życzymy Państwu przyjemnej lektury.

W imieniu Rady Naukowej
Ryszard Bartkowiak
Michał Matusewicz

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 9–30

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

Elżbieta Izabela Szczepankiewicz
Katedra Rachunkowości
Uniwersytet Ekonomiczny w Poznaniu

Zagrożenia dla zasobów informatycznych rachunkowości w dobie transformacji *Information Technology* w jednostkach sektora finansów publicznych

Streszczenie

Ważnym aspektem właściwego poziomu sprawności i jakości działania w jednostkach sektora finansów publicznych jest zapewnienie ciągłości działania systemów informatycznych i bezpieczeństwa zasobów informatycznych. Wykorzystanie systemów informatycznych i techniki teleinformatycznej w tych jednostkach wiąże się z wieloma zagrożeniami związanymi ze środowiskiem informatycznym. W opracowaniu omówiono najważniejsze zagrożenia, które dotyczą tradycyjnego modelu zarządzania zasobami informatycznymi w jednostkach oraz nowego modelu „przetwarzania w chmurze" (ang. *cloud computing*). Poruszono problem zagrożeń i zaprezentowano wnioski z badań w kontekście transformacji technologicznych oraz niedoskonałości systemów kontroli zarządczej, które nie zawsze nadążają za tymi zmianami. Metodą badawczą przyjętą w opracowaniu jest przegląd literatury, przepisów prawnych, standardów kontroli zarządczej, standardów audytu wewnętrznego, norm ISO oraz wnioskowanie.

Słowa kluczowe: rachunkowość, system informatyczny, zagrożenia, bezpieczeństwo zasobów IT, zarządzanie ryzykiem, system kontroli zarządczej, *cloud computing*
Kod klasyfikacji JEL: M15

1. Wprowadzenie

Od wielu lat zarządzanie w jednostkach sektora finansów publicznych (JSFP) wspomagane jest rozwiązaniami i narzędziami informatycznymi. Jednym z najważniejszych aspektów sprawności działania tych jednostek jest zapewnienie ciągłości działania systemów informatycznych rachunkowości oraz wiarygodności i bezpieczeństwa informacji finansowej.

Współczesne uwarunkowania funkcjonowania JSFP powodują, że skuteczne zarządzanie środowiskiem informatycznym w JSFP staje się coraz trudniejsze. Od kilku lat systematycznie rośnie liczba zagrożeń związanych z wykorzystaniem nowych rozwiązań informatycznych i transformacji technologii w tym zakresie. Powszechnie mówi się o różnego rodzaju masowych cyberatakach na publiczne bazy danych, zarówno dużych, jak i małych JSFP[1].

Poza incydentami dotyczącymi bezpieczeństwa informacji w JSFP należy mieć na uwadze także wiele innych czynników ryzyka, które mogą zagrażać pozostałym zasobom w środowisku informatycznym, w tym tych, które są związane z prowadzeniem zinformatyzowanej rachunkowości. Dlatego w ostatnich latach w praktyce sektora finansów publicznych coraz większą uwagę przywiązuje się do poprawienia skuteczności zarządzania ryzykiem w środowisku informatycznym rachunkowości w ramach funkcjonujących w tych jednostkach systemów kontroli zarządczej. Szczególnie ważne dla obszaru funkcjonowania systemów informatycznych rachunkowości w JSFP są zasady i procedury kontroli zarządczej, które dotyczą zapewnienia: poprawności przetwarzania danych finansowych, wiarygodności ksiąg rachunkowych oraz sprawozdań finansowych i budżetowych, a także bezpieczeństwa pozostałych zasobów informatycznych rachunkowości.

[1] Z różnych raportów instytucji specjalistycznych, monitorujących incydenty bezpieczeństwa informatycznego, a także z informacji medialnych, wynika, że wiele JSFP codziennie odnotowuje nawet po kilkanaście lub kilkadziesiąt prób ataków na ich zasoby informacji.

Ze względu na stopień skomplikowania i interdyscyplinarność tematu (wymaga on znajomości organizacji rachunkowości w środowisku informatycznym, różnych zagadnień z zakresu informatyki, zarządzania ryzykiem, właściwej interpretacji wielu różnorodnych tematycznie regulacji w przedmiotowym obszarze) w krajowej literaturze naukowej, poza kilkoma opracowaniami autorki, temat ten jest bardzo rzadko naświetlany. Naukowcy w Polsce nie prowadzili dotychczas badań empirycznych w tym zakresie. Należy podkreślić, że Stowarzyszenie do spraw Audytu i Kontroli Systemów Informatycznych (ISACA) obecnie jest w trakcie opracowywania pierwszego raportu na temat bezpieczeństwa informacji i cyberbezpieczeństwa w jednostkach sektora finansów publicznych, które ma się ukazać w 2017 r. Zatem wiedza teoretyczna i praktyczna pozostaje nadal zasobem prywatnym praktyków w JSFP.

Z powyższych względów podstawowym celem opracowania jest uporządkowanie teoretycznych i praktycznych aspektów wiedzy o elementach środowiska informatycznego rachunkowości oraz o ich podatności na zagrożenia we współczesnej cyberprzestrzeni jednostek funkcjonujących w sektorze finansów publicznych w kontekście realizacji celów kontroli zarządczej[2]. W opracowaniu omówiono najważniejsze czynniki ryzyka w tradycyjnym modelu zarządzania zasobami informatycznymi w JSFP oraz przy wykorzystaniu nowych modeli *cloud computing*. Zaprezentowano również wyniki przeprowadzonych badań empirycznych na temat zagrożeń i oceny stanu ochrony przed nimi w ramach systemów kontroli zarządczej w JSFP.

2. Formalne aspekty zarządzania bezpieczeństwem zasobów informatycznych rachunkowości w jednostkach sektora finansów publicznych

Od wielu lat ogólne zasady bezpieczeństwa zasobów informatycznych oraz zapewnienia wiarygodności przetwarzania danych i informacji finansowej pochodzącej z systemu informatycznego rachunkowości we wszystkich jednostkach, które prowadzą rachunkowość zgodnie z przepisami ustawy o rachunkowości, są regulowane zapisami tejże ustawy. Podstawowe przepisy prawa bilansowego w zakresie ochrony danych i systemu informatycznego rachunkowości dotyczą:

[2] Artykuł powstał w ramach projektu międzyuczelnianego nr 51109-XX4 „Doskonalenie procesów zarządzania ryzykiem w jednostkach sektora finansów publicznych i jednostkach sektora finansowego. Metody, techniki, narzędzia", realizowanego w UE w Poznaniu pod kierownictwem dr E.I. Szczepankiewicz.

- wymagań ochrony danych, które wynikają z art. 10, 13, 23, 24, 71 i 72 ustawy,
- warunków przechowywania ksiąg rachunkowych w formie zbiorów na nośnikach komputerowych określonych w art. 72,
- stosowania zabezpieczeń fizycznych i organizacyjnych w jednostce, których obowiązek wynika z art. 71 ust. 2 ustawy,
- zapewnienia trwałości zapisu danych w systemie informatycznym rachunkowości, które wynika z art. 72 ust. 2 ustawy.

W JSFP zarządzanie środowiskiem informatycznym, w tym środowiskiem zinformatyzowanej rachunkowości, jest uwarunkowane nie tylko przepisami ustawy o rachunkowości, lecz także ustawy o finansach publicznych[3], standardami kontroli zarządczej[4], standardami audytu wewnętrznego[5], a także wieloma innymi przepisami[6] i normami ISO, dotyczącymi bezpieczeństwa informacji[7].

---

[3] Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2013 r., poz. 885 z późn. zm.).

[4] Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz.Urz. Min. Fin. 2009, nr 15, poz. 84).

[5] Komunikat Nr 2 Ministra Finansów z dnia 17 czerwca 2013 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych (Dz.Urz. Min. Fin. z 2013 r., poz. 15).

[6] Do przepisów prawa w tym obszarze należy zaliczyć m.in.: ustawę o ochronie danych osobowych, ustawę o ochronie baz danych, ustawę o świadczeniu usług drogą elektroniczną, ustawę o podpisie elektronicznym, ustawę o ochronie osób i mienia, ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne. Do ustaw wydano także wiele aktów wykonawczych w tym zakresie: rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych; rozporządzenie w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty i warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego; rozporządzenie w sprawie zasad potwierdzania, przedłużania ważności, unieważniania oraz wykorzystania profilu zaufanego elektronicznej platformy usług administracji publicznej; rozporządzenie w sprawie systemów teleinformatycznych stosowanych w jednostkach organizacyjnych pomocy społecznej; rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych; rozporządzenie w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych; rozporządzenie zmieniające rozporządzenie w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych; rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych; rozporządzenie zmieniające rozporządzenie w sprawie określenia rodzajów deklaracji, które mogą być składane za pomocą środków komunikacji elektronicznej; rozporządzenie zmieniające rozporządzenie w sprawie trybu dostępu i wzoru upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz wykorzystywania danych.

[7] Najważniejsze normy ISO w jednostkach sektora finansów publicznych to na przykład: PN-ISO/IEC 17799/2007; PN-ISO/IEC 2382–8:2001; PN-I-02000:2002; PN-ISO/IEC 27001:2007; PN-ISO/IEC 27005:2014–01; PN-ISO/IEC 24762:2010; PN-ISO/IEC 20000–2:2007; PN-ISO/IEC 20000–1:2014–01.

Niewątpliwie, na jakość zarządzania środowiskiem informatycznym w danej JSFP ma także wpływ specyfika organizacji środowiska informatycznego oraz jakość stosowanych środków zabezpieczeń w tej jednostce. Specyfika organizacji środowiska informatycznego w danej jednostce głównie zależy od poziomu skłonności kierownictwa do ryzyka, natomiast jakość zastosowanych środków ochrony uwarunkowana jest zabezpieczeniem (zaplanowaniem i otrzymaniem) na te cele odpowiedniego poziomu środków budżetowych.

3. Elementy środowiska informatycznego rachunkowości

W polskiej literaturze nikt jeszcze nie zdefiniował środowiska informatycznego dla rachunkowości w JSFP ani nie wskazał jej elementów. Pojęcie to również nie zostało dotąd zdefiniowane w żadnych polskich przepisach i standardach dotyczących rachunkowości, standardach rewizji finansowej czy standardach audytu wewnętrznego. Nie zawarto również takiej definicji i nie opisano elementów środowiska informatycznego w standardach kontroli zarządczej, które bezpośrednio dotyczą tego obszaru zarządzania w JSFP. Należy wspomnieć, że w ustawie o rachunkowości ustawodawca używa takich terminów, jak: system informatyczny, system przetwarzania danych, informatyczny nośnik danych, system informatyczny rachunkowości. Terminy te jednak nie zostały zdefiniowane w tym akcie.

Definicję środowiska informatycznego można znaleźć jedynie w Międzynarodowych Standardach Rewizji Finansowej (MSRF)[8] z 1996 r. W myśl MSRF 401[9] środowisko systemów informatycznych istnieje, gdy komputer dowolnego typu i wielkości jest użytkowany do przetwarzania przez jednostkę informacji finansowych znaczących dla badania, niezależnie od tego, czy komputer ten obsługuje jednostka, czy

[8] *Międzynarodowe Standardy Rewizji Finansowej 1996*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 1996.

[9] Należy wspomnieć, że MSRF 401 zawarty w MSRF z 1996 r. usunięto ze struktury MSRF podczas ich aktualizacji w grudniu 2004 r., ale najważniejsze wytyczne z tego standardu zostały włączone w treść innych znowelizowanych standardów oraz nowo przyjętego MSRF 315 oraz *MSRF 315 – Poznanie jednostki i jej środowiska oraz szacowanie ryzyka wystąpienia istotnej nieprawidłowości*, w: *Międzynarodowe Standardy Rewizji Finansowej 2005. Wydanie zbiorcze obejmujące regulacje z zakresu rewizji finansowej, usług atestacyjnych i etyki*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 2005, a następnie zmodyfikowanego w 2009 r. *MSRF 315 Rozpoznanie i ocena ryzyka istotnego zniekształcenia dzięki poznaniu jednostki i jej otoczenia*, w: *Międzynarodowe Standardy Rewizji Finansowej i Kontroli Jakości: 210, 220, 240, 250, 265, 300, 315, 320, 402, 450, 800, 805, 810*, t. 3, IFAC, tłumaczenie: Krajowa Izba Biegłych Rewidentów i Stowarzyszenie Księgowych w Polsce, Warszawa 2010.

strona trzecia[10]. W 2001 r. do zaktualizowanych MSRF dodano *Słownik terminów IT*[11], w którym środowisko IT zdefiniowano jako zasady i procedury wdrożone przez jednostkę, a także infrastrukturę informatyczną, programy (aplikacje) użytkowe i bazy danych przez nią wykorzystywane przy prowadzeniu działalności jednostki.

Zatem należy wnioskować, że w JSFP przetwarzanie danych finansowych z wykorzystaniem oprogramowania dla rachunkowości oznacza, że odbywa się ono w środowisku informatycznym rachunkowości. Rozpatrując strukturę środowiska informatycznego dla systemu rachunkowości, można stwierdzić, że tworzą ją co najmniej takie kategorie, jak:

- zasoby informatyczne wykorzystane do prowadzenia rachunkowości,
- infrastruktura techniczna,
- personel, związany ze środowiskiem informatycznym rachunkowości, który można dzielić według różnych grup zawodowych,
- system organizacji pracy w jednostce,
- elementy otoczenia zewnętrznego.

W każdej z wyżej wymienionych kategorii związanej ze środowiskiem informatycznym rachunkowości można wskazać wiele elementów szczegółowych, które są z nimi związane. Przykładowo do zasobów informatycznych w JSFP zaliczyć należy przede wszystkim[12]:

- sprzęt komputerowy, tj. komputery, serwery, monitory, drukarki, modemy, skanery itd.,
- oprogramowanie systemowe, np. system operacyjny, system zarządzania bazą danych, narzędzia systemowe, programy diagnostyczne,
- oprogramowanie użytkowe uniwersalne, np. arkusze kalkulacyjne, edytory tekstów,
- oprogramowanie specjalne, czyli aplikacje użytkowe, w tym podsystemy dziedzinowe rachunkowości (np. system finansowo-księgowy, system gospodarki magazynowej, system kadrowo-płacowy),
- zbiory (bazy) danych, w tym bieżące kopie bezpieczeństwa danych oraz kopie ksiąg rachunkowych,

---

[10] Paragraf 1 *MSRF 401 – Badanie w środowisku komputerowych systemów informacyjnych*, w: *Międzynarodowe Standardy Rewizji Finansowej i Międzynarodowe Wskazówki dotyczące Praktyki Rewizji Finansowej 2001*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 2001, s. 187.

[11] *Słownik terminów IT*, w: *Międzynarodowe Standardy Rewizji*…, op.cit., s. 720.

[12] E.I. Szczepankiewicz, *Audyt sprawozdań finansowych w środowisku informatycznym*, w: *Audyt sprawozdań finansowych*, red. W. Gabrusewicz, PWE, Warszawa 2010, s. 198.

- nośniki danych,
- dokumentację projektową rozwiązań informatycznych, w tym rozwoju (i/lub aktualizacji funkcji) systemu informatycznego rachunkowości,
- dokumentację ewidencyjną systemu informatycznego rachunkowości,
- dokumentację dla użytkowników systemu informatycznego rachunkowości.

Infrastrukturę techniczną w JSFP tworzą systemy zasilania, chłodzenia, klimatyzacji, ochrony przeciwpożarowej, sieci teletransmisyjne i centra administracyjne systemu, systemy (procedury) ochrony dostępu fizycznego do zasobów informatycznych itp.[13].

Personel związany ze środowiskiem informatycznym rachunkowości w JSFP można dzielić według grup zawodowych, czyli są to: użytkownicy podsystemów rachunkowości (tj. osoby prowadzące ewidencję operacji, inne osoby kadry księgowej, kierowniczej, osoba administrująca uprawnieniami użytkowników), projektanci systemów informatycznych, programiści systemów informatycznych, oficer bezpieczeństwa, zewnętrzni programiści podsystemów rachunkowości, administratorzy systemów i/lub baz danych, serwisanci sprzętu komputerowego, serwisanci oprogramowania, osoby odpowiedzialne za dystrybucję i bezpieczeństwo nośników danych[14].

Mając na uwadze system organizacji pracy w JSFP, mówimy o scentralizowanym lub rozproszonym przetwarzaniu danych, które jest realizowane we własnym zakresie przez jednostkę, albo o powierzeniu prowadzenia rachunkowości innej jednostce (może to dotyczyć małych JSFP), a także o korzystaniu z usług specjalistycznych centrów administrowania danymi. Z tym zagadnieniem wiąże się odpowiednia organizacja systemu kontroli zarządczej w danej JSFP i podział odpowiedzialności za kontrolę nad zasobami informatycznymi.

Do elementów otoczenia zewnętrznego, który ma wpływ na zakres procedur kontroli zarządczej w JSFP, zaliczyć należy co najmniej[15]:

- organizację przetwarzania danych przy powierzeniu prowadzenia rachunkowości lub przetwarzania innych danych jednostce zewnętrznej,

---

[13] E.I. Szczepankiewicz, *Zasady i procedury kontroli zarządczej w obszarze systemów informatycznych rachunkowości w jednostkach sektora finansów publicznych*, Wydawnictwo Naukowe CONTACT, Poznań 2016, s. 19.

[14] E.I. Szczepankiewicz, *Kontrola zarządcza w jednostkach samorządu terytorialnego. Doskonalenie procedur kontroli zarządczej w środowisku informatycznym rachunkowości*, Wydawnictwo Naukowe CONTACT, Poznań 2016, s. 28.

[15] E.I. Szczepankiewicz, *Audyt sprawozdań finansowych w środowisku informatycznym*, w: *Audyt sprawozdań finansowych. Teoria i praktyka*, red. W. Gabrusewicz, PWE, Warszawa 2014, s. 232.

- organizację przekazywania danych pomiędzy jednostkami sektora publicznego lub między JSFP a inną jednostką zewnętrzną (forma tradycyjna lub przy użyciu łącz transmisyjnych, np. przez Internet),
- podział odpowiedzialności za kontrolę i bezpieczeństwo danych między stronami powyższych umów.

Wyżej wymienione elementy szczegółowe środowiska informatycznego rachunkowości występują w mniejszym lub większym zakresie w każdej JSFP, niezależnie od jej formy organizacyjnej, wielkości, zakresu realizowanych zadań publicznych czy specyfiki działania. Powyższe elementy środowiska informatycznego są charakterystyczne także dla innych jednostek gospodarczych w sektorze prywatnym.

4. Czynniki ryzyka w środowisku informatycznym rachunkowości

Cechy środowiska informatycznego oraz podatność jego poszczególnych elementów na różnego typu zagrożenia w JSFP wiążą się z jakością wykorzystywanego systemu informatycznego rachunkowości, a także z charakterem organizacji systemu rachunkowości oraz systemu kontroli zarządczej w jednostce.

W JSFP zwraca się szczególną uwagę na te elementy środowiska informatycznego i zagrożenia z nimi związane, które mogą wywoływać negatywne efekty dla prawidłowego działania i bezpieczeństwa zasobów informatycznych rachunkowości oraz bezpieczeństwa informacji w publicznych bazach danych. Źródłami ryzyka w JSFP mogą być różne elementy środowiska informatycznego[16]. Jak wyżej wskazano, mogą to być poszczególne elementy zasobów informatycznych, personel księgowy i informatyczny, sposób organizacji pracy i kontroli, a także otoczenie zewnętrzne. Należy jednak pamiętać o tym, że nie wszystkie zagrożenia związane z poszczególnymi elementami środowiska informatycznego w jednakowy sposób mogą oddziaływać

[16] Szerzej o zagrożeniach w środowisku informatycznym: E. Dudek, *Zagrożenia występujące w środowisku informatycznym rachunkowości*, „Monitor Rachunkowości i Finansów" 2003, nr 7–8, s. 45–52; E.I. Szczepankiewicz, M. Dudek, *Rozwój technologii informatycznych a zagrożenia i zarządzanie bezpieczeństwem informacji w przedsiębiorstwach*, w: *Logistyka – Komunikacja – Bezpieczeństwo, Wybrane problemy*, red. M. Grzybowski, J. Tomaszewski, Wydawnictwo Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni, Gdynia 2009, s. 263–274.

na bezpieczeństwo zasobów informatycznych i prawidłowe funkcjonowanie systemu informatycznego rachunkowości[17].

Czynniki ryzyka w środowisku informatycznym teoretycy najczęściej klasyfikują według rodzajów oraz według skutków[18]. Wielu autorów wskazuje, że dane zagrożenie może być spowodowane przez: działanie czynników środowiska naturalnego (zdarzenia losowe) oraz przypadkowe lub celowe działania człowieka, które w efekcie spowodują szkody w zasobach informatycznych jednostki. Zdarzenia losowe, a także przypadkowe lub celowe działania ludzi mogą być pochodzić zarówno z wewnątrz, jak i z zewnątrz jednostki. Zatem na środowisko informatyczne rachunkowości w JSFP mogą mieć wpływ różne wewnętrzne i zewnętrzne czynniki ryzyka.

Wiele wyników badań wskazuje, że pomimo zmieniających się warunków otoczenia i postępu technologii w dziedzinie informatyki, głównym źródłem ryzyka w JSFP, podobnie jak w innych jednostkach gospodarczych, są ludzie związani z systemem informatycznym rachunkowości lub z jego otoczeniem, którzy bezpośrednio lub pośrednio, przypadkowo lub umyślnie wpływają na działanie systemu i/lub bezpieczeństwo informacji[19].

Do celowych działań człowieka przeciwko zasobom informatycznym zgodnie z klasyfikacją normy ISO/IEC TR 13335–3 zalicza się m.in.: zalanie, pożar, umyślną szkodę lub zniszczenie, awarię klimatyzacji, ekstremalną temperaturę i wilgotność, promieniowanie elektromagnetyczne, kradzież, nieuprawnione użycie nośników, błędy personelu obsługującego / użytkowników, nielegalne używanie oprogramowania, błąd konserwacji/serwisu oprogramowania, awarię oprogramowania, użycie oprogramowania przez nieuprawnionych użytkowników, sfałszowanie tożsamości użytkownika, instalację złośliwego oprogramowania, dostęp do sieci nieuprawnionych użytkowników, użycie instalacji sieciowych w nieuprawniony sposób, uszkodzenie linii telekomunikacyjnych, przeciążenie ruchem, podsłuch, infiltrację łączności, analizę ruchu, przekierowanie wiadomości, zaprzeczenie, awarię usług łączności (np. usług sieciowych), niewłaściwe wykorzystanie zasobów informatycznych, a nawet atak terrorystyczny czy użycie broni do zniszczenia zasobów informatycznych.

---

[17] E.I. Szczepankiewicz, *Audyt sprawozdań finansowych w środowisku informatycznym*, w: *Audyt sprawozdań finansowych. Teoria i praktyka*…, op.cit., s. 234.

[18] Klasyfikacje zagrożeń według tych kryteriów proponują na przykład: R.P. Fisher, *Information Systems Security*, Prentice-Hall, Englewood Cliffs 1984, s. 54; T. Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Helion, Gliwice 1999, s. 24–25.

[19] Szerzej szczegółowe wyniki badań o zagrożeniach w środowisku informatycznym rachunkowości prezentują: E.I. Szczepankiewicz, M. Dudek, *Rozwój technologii*…, op.cit., s. 263–274.

Szczególną kategorią celowego działania w środowisku informatycznym JSFP jest przestępczość komputerowa, prowadząca do naruszenia bezpieczeństwa zasobów informatycznych. Działania przestępcze mogą być skierowane przeciwko dostępności informacji, integralności lub jej poufności. Są to na przykład takie działania, jak: haking, fishing, rozpowszechnianie wirusów, niszczenie informacji, wandalizm, kradzież danych lub sprzętu, wewnętrzny lub zewnętrzny sabotaż komputerowy, oszustwo komputerowe, fałszerstwo komputerowe, szpiegostwo komputerowe, podsłuch komputerowy, nielegalne uzyskiwanie i wykorzystywanie programu. Zazwyczaj większość tych działań pochodzi z zewnątrz JSFP. Działania te znalazły odzwierciedlenie w przepisach prawa karnego i prawa o wykroczeniach[20].

Podstawowe zagrożenia dotyczące tradycyjnego modelu zarządzania zasobami informatycznymi, czyli takiego, gdzie JSFP posiada własną infrastrukturę informatyczną i na bieżąco sama utrzymuje ciągłość działania sprzętu komputerowego, w tym serwerów (zasilanie, chłodzenie, serwisowanie itp.), oprogramowania, infrastruktury sieciowej, dotyczą niedoskonałości systemu kontroli zarządczej. Zagrożenia te można podzielić na kilka grup.

Pierwszą grupę zagrożeń stanowią braki i/lub niedoskonałości w zakresie stosowanych zabezpieczeń fizycznych, technicznych i programowych dla zasobów informatycznych i/lub brak ubezpieczenia tych zasobów od zdarzeń losowych. W tej grupie ważne są również aspekty zabezpieczenia się przed zagrożeniami, wynikającymi z niewłaściwej konfiguracji lub stosowania nieodpowiednich zabezpieczeń, dotyczących lokalnych sieci komputerowych w jednostce. Jest to zagrożenie występujące najczęściej w mniejszych JSFP. Błędy i braki w tym zakresie mogą prowadzić m.in. do wewnętrznych i zewnętrznych nadużyć czy przestępstw komputerowych.

Drugą grupę czynników ryzyka w JSFP stanowią braki i/lub niedoskonałe wewnętrzne procedury organizacyjno-administracyjne, które mogą być wykorzystywane przez pracowników do celowych, wewnętrznych naruszeń wobec zasobów informatycznych. W JSFP, podobnie jak w innych jednostkach gospodarczych, bezpośrednio na środowisko informatyczne rachunkowości negatywnie mogą oddziaływać użytkownicy podsystemów informatycznych rachunkowości (kierownictwo, kasjerzy, pozostały personel księgowy), zatrudnieni w jednostce programiści itd. Może to być każda osoba, która uczestniczy w funkcjonowaniu (eksploatacji) systemu,

[20] J.W. Wójcik, *Przestępstwa komputerowe*, cz. 1, *Fenomen cywilizacji*, CIM, Warszawa 1999; J.W. Wójcik, *Przestępstwa komputerowe*, cz. 2, *Techniki zapobiegania*, CIM, Warszawa 1999; K. Mitnick, W. Simon, *Łamałem ludzi, nie hasła. Sztuka podstępu*, Helion, Gliwice 2002; Ustawa z 6 czerwca 1997 r. Kodeks karny (Dz.U. z 1997 r., nr 55, poz. 553 z późn. zm.).

dokładnie znająca ten system oraz niedoskonałości mechanizmów kontroli. Mogą to być także osoby działające indywidualnie lub w zmowie, które mogą zmodyfikować programy albo dane podczas ich wprowadzania i/lub przechowywania. Niebezpieczeństwo takie istnieje szczególnie wtedy, gdy nie występuje skuteczna kontrola zarządcza oparta na właściwym podziale: upoważnień, autoryzacji, funkcji i zadań w strukturze organizacyjnej JSFP.

Groźnym zagrożeniem dla wiarygodności systemu informatycznego rachunkowości w JSFP może być fakt pominięcia testowania systemu informatycznego rachunkowości przed przyjęciem go do eksploatacji, w szczególności w przypadku rozwiązania indywidualnie zamawianego przez jednostkę. Brak takiego testowania stanowi dodatkowy element ryzyka pojawienia się błędów w późniejszym przetwarzaniu danych i sprawozdawczości w jednostce.

Kolejnym bardzo ważnym czynnikiem ryzyka jest brak zaprogramowanych automatycznych procedur kontrolnych w systemach (aplikacjach) użytkowych. W praktyce JSFP systemy informatyczne rachunkowości, w zależności od ceny i klasy systemu, mają bardzo różny poziom i liczbę zaprogramowanych procedur kontrolnych. Niewątpliwie procedury kontroli zarządczej[21] w systemie informatycznym rachunkowości mogą i powinny być realizowane programowo. Jeśli przewidzi się odpowiednie mechanizmy kontroli, w zbiorach danych zapisywane są tylko operacje spełniające warunki kontroli, natomiast treści błędne są na ogół odrzucane przez system już na etapie wprowadzania danych do komputerowego dokumentu księgowego. Ponadto użytkownik, obsługując system informatyczny rachunkowości z zaprogramowanymi kontrolami poprawności wprowadzania danych, może na bieżąco uzyskiwać pomoc (podpowiedzi) ze strony systemu podczas ewidencji operacji księgowych i korzystać z wcześniej wprowadzonych do systemów wzorców księgowań[22].

Wraz z rozwojem JSFP może zaistnieć konieczność zainwestowania w dodatkową infrastrukturę informatyczną. Wówczas jednostka powinna rozważyć, czy nadal będzie tradycyjnie zarządzać swoimi zasobami informatycznymi, ponosząc pełne koszty z tym związane, czy może będzie korzystać z tzw. modelu „przetwarzania

[21] Szerzej o procedurach kontrolnych E.I. Szczepankiewicz, *Wybrane procedury kontroli wewnętrznej w środowisku informatycznym rachunkowości*, w: *Rachunkowość w teorii i praktyce*, t. I, *Rachunkowość finansowa*, red. W. Gabrusewicz, Wydawnictwo Akademii Ekonomicznej w Poznaniu, Poznań 2007, s. 360–376; E.I. Szczepankiewicz, *Jakie są zasady opracowywania procedur kontrolnych w firmie*, „Biuletyn Rachunkowości" 2008, nr 12(60), s. 58–60.

[22] Szerzej E. Dudek, *Zagrożenia*…, op.cit., s. 46.

w chmurze" (ang. *cloud computing*). Należy przewidzieć, że nowe rozwiązania technologiczne operujące w cyberprzestrzeni, pomimo że są tańsze niż utrzymywanie własnej pełnej infrastruktury i personelu informatycznego, będą źródłem dodatkowych nowych zagrożeń dla zasobów informatycznych jednostki.

Przetwarzanie w chmurze to świadczenie określonych, specjalistycznych usług informatycznych za pośrednictwem infrastruktury sieciowej (Internetu). Jest to usługa przetwarzania danych. Poprzez dostęp sieciowy usługodawca na bieżąco (*online*) dostarcza usługobiorcom współdzielony z wieloma usługobiorcami zestaw zasobów przetwarzania, czyli sieci, serwery, przestrzeń do składowania danych, oprogramowanie i usługi z tym związane. Zatem „chmurę" stanowi cały zbiór serwerów, oprogramowania, światłowodów itd., do którego uzyskuje się dostęp za pośrednictwem Internetu. Korzystanie z takiej chmury nazywa się „przetwarzaniem w chmurze"[23]. Usługobiorca, korzystając z tej usługi, nie musi mieć wiedzy technicznej o tym, w jaki sposób odbywa się cały proces dostarczania usługi. Nie wie również, w której części globu fizycznie znajdują się poszczególne elementy całej zaawansowanej technologicznie infrastruktury informatycznej dla tej usługi, w tym: serwery z zasobami informacyjnymi, z których on na co dzień korzysta. Usługa przetwarzania w chmurze ma charakter mierzalny (liczba przesłanych bajtów, czas korzystania itp.). Dlatego usługobiorca płaci tylko za rzeczywiste korzystanie z zasobów[24].

W zależności od stopnia zaawansowania *cloud computing* rozróżnia się obecnie trzy podstawowe rodzaje/poziomy tej usługi:

1. *Infrastructure as a Service* (IaaS);
2. *Platform as a Service* (PaaS);
3. *Software as a Service* (SaaS).

W tabeli 1 zamieszczono podstawową charakterystykę przetwarzania w chmurze według stopnia zaawansowania usług nabywanych przez JSFP.

Udział w tematycznych konferencjach oraz badania własne autorki potwierdziły, że kierownicy JSFP, księgowi i audytorzy od kilku lat bardzo uważnie obserwują dynamiczny rozwój tego typu usług informatycznych. JSFP mają już świadomość, że decydując się na określony model *cloud computing*, muszą przyjąć na siebie ściśle

[23] P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, Ver. 15, 10.07.2009 r., http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, dostęp 15.05.2015; K. Łapiński, B. Wyżnikiewicz, *Raport. Cloud Computing wpływ na konkurencyjność przedsiębiorstw i gospodarkę Polski*, Instytut Badań nad Gospodarką Rynkową, Warszawa 2011, s. 5–20.

[24] E.I. Szczepankiewicz, *Audyt kontroli wewnętrznej rachunkowości w środowisku informatycznym*, Difin, Warszawa 2016, s. 66–67.

określony podział między stronami kontroli nad wykorzystywanymi zasobami informatycznymi w chmurze. Podział kontroli zazwyczaj określa usługodawca. W praktyce JSFP rzadko mają możliwość współdecydowania o zakresie podziału kontroli nad swoimi danymi i wykorzystywanymi zasobami informatycznymi. Należy podkreślić, że w tradycyjnym modelu zarządzania zasobami informatycznymi JSFP sprawuje niemal całkowitą kontrolę nad posiadaną przez siebie infrastrukturą, oprogramowaniem i danymi. Jej samowystarczalność i pełna kontrola nad zasobami informatycznymi może być jedynie w niewielkim stopniu ograniczona koniecznością korzystania z usług dostawców łączy internetowych czy serwisu informatycznego.

Tabela 1. Charakterystyka usług *cloud computing*

Usługa	Podstawowa charakterystyka
Infrastructure as a Service	JSFP korzysta za pośrednictwem Internetu z infrastruktury i sprzętu informatycznego (ang. *hardware*). Takim sprzętem może być przestrzeń na wirtualnym dysku internetowym przeznaczona do przechowywania danych albo też wydzierżawione na serwerze miejsce w celu umieszczenia na nim na przykład strony internetowej. Do IaaS zalicza się także korzystanie z mocy obliczeniowej procesorów. W razie potrzeby przeprowadzenia jednorazowej operacji wymagającej ponadstandardowej mocy JSFP może mieć zapewniony dostęp do wirtualnego superkomputera, na który składają się setki połączonych ze sobą procesorów
Platform as a Service	Dla JSFP usługa PaaS jest bardziej zaawansowanym poziomem usługi przetwarzania w chmurze niż usługa IaaS. W tym przypadku JSFP oprócz dostępu do infrastruktury otrzymuje także dostęp do środowiska (w tym platformy programistycznej), w którym może sobie instalować i uruchamiać nowe aplikacje informatyczne. Prostym przykładem takiego środowiska jest system operacyjny Windows. JSFP mogłaby łączyć się poprzez Internet z komputerem, na którym byłby zainstalowany określony system operacyjny i miałaby dostęp do usługi PaaS, czyli mogłaby instalować niezbędne aplikacje. W modelu PaaS instalowane aplikacje pozostają własnością usługobiorcy
Software as a Service	Usługa SaaS dla JSFP jest najbardziej rozbudowanym poziomem *cloud computing*. W modelu tym, oprócz infrastruktury sprzętowej wraz z zawartym środowiskiem operacyjnym, JSFP otrzymuje także dostęp do określonych aplikacji informatycznych, oferowanych przez usługodawcę. Mogą to być proste programy, jak np. edytor tekstu *online*, a także bardziej zaawansowane aplikacje, np. systemy do obsługi księgowości, poczty elektronicznej, rozliczania zamówień. Wówczas JSFP wykorzystuje oprogramowanie należące do usługodawcy, który odpowiada za jego aktualizację i bezawaryjne działanie

Źródło: opracowanie własne na podstawie P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, Ver. 15, 10.07.2009 r., http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf; *The 2011 Cloud Dividend Report*, http://uk.emc.com/microsites/2010/cloud-dividend/index.htm; F. Etro, *Introducing Cloud Computing. Results from a Simulation Study*, International Think-tank on Innovation and Competition, November 2010; P. Dzwonkowski, *Ryzyka związane z usługą przetwarzania danych w chmurze i metody ich łagodzenia*, prezentacja na konferencję „Bezpieczeństwo i Ochrona Danych w Modelu *Cloud Computing*" z dnia 30 marca 2011 r.; K. Łapiński, B. Wyżnikiewicz, *Raport. Cloud Computing wpływ na konkurencyjność przedsiębiorstw i gospodarkę Polski*, Instytut Badań nad Gospodarką Rynkową, Warszawa 2011, s. 5–20.

Zatem wybór odpowiedniego modelu przetwarzania w chmurze to wybór pomiędzy stopniem kontroli nad zasobami informatycznymi JSFP a stopniem efektywności ekonomicznej jej działania. Przykładowo, JSFP decydująca się na model *Software as a Service*, nie będzie ponosić kosztów zakupów i utrzymania rozbudowanej infrastruktury informatycznej, ale jej działalność operacyjna jest niemal całkowicie uzależniona od jakości usług dostawcy chmury. Pomimo niższych kosztów zarządzania zasobami informatycznymi przy wykorzystaniu technologii *cloud computing* znacznie rośnie liczba czynników ryzyka dla JSFP.

Stopień zaawansowania przetwarzania w chmurze ma także drugi wymiar, związany z poziomem zarządzania zasobami w chmurze przez usługobiorcę, czyli JSFP. Teoretycy wyróżniają trzy podstawowe modele zarządzania zasobami informatycznymi przez jednostkę w chmurze. Mówi się o modelach:

1) chmury prywatnej,
2) chmury publicznej,
3) chmury hybrydowej.

W praktyce powyższy podział usług przetwarzania w chmurze, zarówno pod względem stopnia zaawansowania nabywanych usług oraz kontroli nad zasobami, jak i fizycznego umiejscowienia chmury (serwery fizycznie zazwyczaj znajdują się w innych krajach), nie jest tak sztywny i nie ogranicza się tylko do trzech modeli wymienianych przez teoretyków. Konieczność dostosowywania się do potrzeb potencjalnego usługobiorcy spowodowała, że obecnie bardzo często są oferowane rozwiązania mieszane. Jednym z takich rozwiązań jest czwarty model wymieniony w tabeli 2, czyli chmura dedykowana, która wykształciła się z modelu chmury hybrydowej. Z usług chmury dedykowanej coraz powszechniej korzystają zarówno jednostki administracji rządowej, jak i jednostki administracji samorządowej.

W tabeli 2 zawarto charakterystykę modeli zarządzania zasobami informatycznymi przez JSFP w chmurze prywatnej, publicznej, hybrydowej i dedykowanej.

Dla osób odpowiedzialnych za rachunkowość JSFP przekazanie niemal całkowitej kontroli nad własnymi zasobami informatycznymi usługodawcom zewnętrznym staje się obecnie warunkiem trudnym do zaakceptowania. Jak potwierdzają wyniki badań przeprowadzonych przez autorkę w 2014 r.[25], osoby odpowiedzialne za rachunkowość nie akceptowały przyjęcia w swoich jednostkach do zarządzania

[25] Badania własne autorka przeprowadziła 25.02.2014 r. podczas konferencji dla członków Stowarzyszenia Księgowych w Polsce, Oddział w Poznaniu, pt.: „Księgowy w epicentrum zmian w VAT, cyfryzacji i globalizacji – wyzwania roku 2014", organizator: Stowarzyszenie Księgowych w Polsce, Oddział w Poznaniu i enova dla biznesu.

zasobami informatycznymi rachunkowości modelu chmury publicznej. Zaledwie 8,5% księgowych deklarowało, że w przyszłości rozważy model chmury dedykowanej lub chmury prywatnej.

Tabela 2. Charakterystyka modeli zarządzania zasobami informatycznymi w chmurze przez JSFP

Usługa	Podstawowa charakterystyka
Chmura prywatna	Całość infrastruktury informatycznej znajduje się fizycznie na terenie kontrolowanym przez JSFP. Jednostka ma więc przez cały czas bezpośredni dostęp do zasobów przechowywanych danych na własnych serwerach posiadających oprogramowanie tworzące chmurę prywatną JSFP. Środowisko informatyczne, w tym oprogramowanie, jest zazwyczaj dopasowane indywidualnie do potrzeb JSFP, która może posiadać wyłączny dostęp do oferowanych w chmurze usług
Chmura publiczna	JSFP w całości może korzystać z zewnętrznych zasobów informatycznych. JSFP sama decyduje, z których usług oferowanych przez usługodawcę będzie korzystać. Jednocześnie JSFP może korzystać za pośrednictwem dostawcy chmury z usług podmiotów trzecich, które nie są bezpośrednim dostawcą chmury, ale dostarczają np. specjalne oprogramowanie, które instaluje się w udostępnionym środowisku operacyjnym dla obsługi chmury. Aspekt braku możliwości kontroli zasobów danych rachunkowości w „chmurze publicznej" przez JSFP obecnie zniechęca księgowych do interesowania się tą usługą. Decydują o tym takie czynniki, jak brak informacji o fizycznym umiejscowieniu chmury (serwery w dowolnym kraju na świecie), a w konsekwencji różne systemy prawne ochrony zasobów informacyjnych i usługobiorców w tych krajach
Chmura hybrydowa	Rozwiązanie to polega na wykorzystywaniu części zasobów informatycznych i przechowywaniu danych w „chmurze prywatnej", a w części w „chmurze publicznej". W „chmurze prywatnej" JSFP przetwarza zazwyczaj na własnych zasobach dane strategiczne i dane prawnie chronione (np. dane niejawne) jednostki. Do „chmury publicznej" JSFP przenosi tylko te aplikacje użytkowe, za pośrednictwem których przetwarza pozostałe dane
Chmura dedykowana w modelu chmury hybrydowej	Jednostka może wykorzystać pełną funkcjonalność chmury w sposób wysoce dopasowany do jej specyficznych potrzeb. Usługodawca dla takiej JSFP wyodrębnia wówczas pewną część chmury (są to specjalnie wydzielone serwery), do której wyłączny dostęp ma tylko ta konkretna JSFP

Źródło: opracowanie własne.

Wyniki uzyskane na podstawie odpowiedzi z ankiet skierowanych przez autorkę do księgowych (67% ankietowanych księgowych zatrudnionych było w sektorze prywatnym i 33% w sektorze finansów publicznych) przedstawiają się następująco:

– tylko 23% ankietowanych księgowych w sektorze prywatnym oraz 49% w JSFP w udokumentowany sposób identyfikuje i ocenia zagrożenia informatyczne, które mogą przeszkodzić realizacji celów i zadań komórki finansowo-księgowej

(np. poprzez sporządzanie rejestru ryzyka, wymaganego standardami kontroli zarządczej w JSFP);
- tylko 19% ankietowanych księgowych w sektorze prywatnym oraz 35% w JSFP potwierdziło, że w przypadku każdego zagrożenia/ryzyka informatycznego został określony poziom ryzyka, jaki można zaakceptować w ich jednostkach;
- 14% ankietowanych księgowych w sektorze prywatnym oraz 44% w JSFP odpowiedziało, że w stosunku do każdego istotnego ryzyka informatycznego został określony sposób radzenia sobie z tym ryzykiem (tzn. zdefiniowano i wdrożono reakcję na ryzyko, wymaganą standardami kontroli zarządczej w JSFP);
- 52% ankietowanych księgowych w sektorze prywatnym oraz 72% w JSFP stwierdziło, że pracownicy w komórce finansowo-księgowej mają bieżący dostęp do procedur/instrukcji ochrony zasobów informatycznych obowiązujących w jednostce (np. poprzez intranet);
- 49% ankietowanych księgowych w sektorze prywatnym oraz 79% w JSFP zapewniało, że w ich jednostkach zostały wdrożone mechanizmy (procedury), służące utrzymaniu ciągłości działalności na wypadek awarii systemu informatycznego oraz zdarzeń losowych związanych z utratą lub zniszczeniem zasobów informatycznych (np. pożaru, powodzi, zalania);
- około 72% wszystkich ankietowanych księgowych uważa, że dokumenty i inne zasoby informatyczne, z których korzystają w swojej pracy, są ich zdaniem chronione przed utratą lub zniszczeniem zgodnie z przepisami;
- 86% ankietowanych księgowych w JSFP oraz 83% w sektorze prywatnym z pośród wszystkich zagrożeń dla bezpieczeństwa informacji najbardziej obawia się prób wyłudzeń danych przez osoby z zewnątrz, w celu dokonywania przelewów z kont jednostki, działań znanych jako *phishing* oraz *spyware*, rozproszonego ataku DoS, w dalszej kolejności ataku wirusów i innych szkodliwych programów, włamania z zewnątrz w celu kradzieży poufnych danych i danych osobowych z publicznych (firmowych) baz danych;
- około 27% wszystkich ankietowanych księgowych za ważne zagrożenia dla bezpieczeństwa (utraty lub zniszczenia) zasobów informatycznych rachunkowości uważa możliwość awarii infrastruktury, sprzętu komputerowego (dysków, serwerów) lub oprogramowania.

Na podstawie kolejnych badań ankietowych przeprowadzonych przez autorkę na przełomie lat 2015–2016 można stwierdzić, że pracownicy w większości badanych JSFP (69% ankietowanych), a w szczególności mniejszych i średnich JSFP (aż 92% ankietowanych) dostrzegli, że aktualnie obowiązujące rozwiązania w systemach

kontroli zarządczej w ich jednostkach nie nadążają za transformacją technologiczną w obszarze IT. Skutkiem tego w wielu obszarach środowiska informatycznego nie zapewniono na właściwym poziomie bezpieczeństwa zasobów informatycznych. Zdaniem 93% ankietowanych w JSFP istnieje niebezpieczeństwo, że podatności na zagrożenia w ich jednostkach w przyszłości mogą zostać wykorzystane przez celowe działania z zewnątrz jednostki. Ponadto w 12% badanych jednostek zdaniem ankietowanych istnieje ryzyko wyrządzenia szkód zasobom informatycznym w wyniku ewentualnych zdarzeń losowych.

5. Podsumowanie

Przegląd literatury[26], analiza regulacji oraz badania empiryczne przeprowadzone przez autorkę potwierdziły, że organizacja i zarządzanie bezpieczeństwem środowiska informatycznego rachunkowości oraz opracowanie, wdrożenie, ocena i doskonalenie systemu kontroli zarządczej w JSFP stanowią obecnie bardzo złożony obszar działań.

Zaprezentowane zagrożenia i wielość czynników je wywołujących pokazują, że obecnie ze względu na dynamiczną transformację technologiczną liczba elementów środowiska informatycznego, które wywołują różne zagrożenia w JSFP, jest coraz większa. Zależnie od przyjętego modelu zarządzania zasobami informatycznymi (model tradycyjny lub model *cloud computing*) kierownictwo JSFP musi uświadomić sobie i przeanalizować znacznie różniące się czynniki ryzyka, które mogą wystąpić w danym środowisku informatycznym i nie może ich zlekceważyć podczas doskonalenia systemu kontroli zarządczej. Kierownictwo JSFP powinno przewidzieć i przeciwdziałać ryzyku, stosując odpowiednie mechanizmy kontroli zarządczej[27], które będą chronić na możliwie najwyższym poziomie zasoby informatyczne przed zagrożeniami, a w konsekwencji przed ich utratą. Wszystkie wyżej omówione czynniki i okoliczności uzasadniają potrzebę bardzo dokładnej analizy podatności poszczególnych elementów na zagrożenia, a także potrzeb jednostki i oczekiwań wobec roli

[26] Literatura zagraniczna nie odnosi się do aspektów kontroli zarządczej w polskim sektorze finansów publicznych. Istnieje natomiast wiele opracowań i specjalistycznych raportów zagranicznych omawiających różne aspekty bezpieczeństwa informacji oraz cyberbezpieczeństwa w szeroko rozumianych organizacjach.

[27] Szerzej o analizie ryzyka dla potrzeb projektowania systemu kontroli E.I. Szczepankiewicz, *Analiza ryzyka jako element systemu kontroli w firmie*, „Biuletyn Rachunkowości" 2008, nr 14.

oraz zadań systemu kontroli zarządczej w środowisku informatycznym rachunkowości. Przy opracowywaniu zasad i środków bezpieczeństwa zasobów informatycznych analizą należy objąć wszystkie wewnętrzne oraz zewnętrzne czynniki ryzyka, które są specyficzne dla danej JSFP[28]. W następstwie przeprowadzonej analizy kierownictwo JSFP powinno przyjąć odpowiednią politykę zarządzania ryzykiem i zasobami w środowisku informatycznym.

Bibliografia

1. Dudek E., *Zagrożenia występujące w środowisku informatycznym rachunkowości*, „Monitor Rachunkowości i Finansów" 2003, nr 7–8.
2. Dzwonkowski P., *Ryzyka związane z usługą przetwarzania danych w chmurze i metody ich łagodzenia*, prezentacja na konferencję „Bezpieczeństwo i Ochrona Danych w Modelu *Cloud Computing*" z dnia 30 marca 2011 r.
3. Etro F., *Introducing Cloud Computing. Results from a Simulation Study*, International Think-tank on Innovation and Competition, November 2010.
4. Fisher R.P., *Information Systems Security*, Prentice-Hall, Englewood Cliffs 1984.
5. Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Helion, Gliwice 1999.
6. Komunikat nr 2 Ministra Finansów z dnia 17 czerwca 2013 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych (Dz.Urz. Min. Fin. z 2013 r., poz. 15).
7. Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz.Urz. Min. Fin. 2009, nr 15, poz. 84).
8. Łapiński K., Wyżnikiewicz B., *Raport. Cloud Computing wpływ na konkurencyjność przedsiębiorstw i gospodarkę Polski*, Instytut Badań nad Gospodarką Rynkową, Warszawa 2011.
9. Mell P., Grance T., *The NIST Definition of Cloud Computing*, Ver. 15, 10.07.2009 r., http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, dostęp 15.05.2015.
10. *Międzynarodowe Standardy Rewizji Finansowej 1996,* IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 1996.
11. *Międzynarodowe Standardy Rewizji Finansowej 2005. Wydanie zbiorcze obejmujące regulacje z zakresu rewizji finansowej, usług atestacyjnych i etyki*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 2005.

[28] Szerzej o tym ryzyku: E.I. Szczepankiewicz, *Jak chronić dane finansowe w środowisku informatycznym rachunkowości*, „Biuletyn Rachunkowości i Finansów" 2007, nr 8(32), s. 61–64.

12. *Międzynarodowe Standardy Rewizji Finansowej i Kontroli Jakości: 210, 220, 240, 250, 265, 300, 315, 320, 402, 450, 800, 805, 810*, t. 3, IFAC, tłumaczenie: Krajowa Izba Biegłych Rewidentów i Stowarzyszenie Księgowych w Polsce, Warszawa 2010.
13. *Międzynarodowe Standardy Rewizji Finansowej i Międzynarodowe Wskazówki dotyczące Praktyki Rewizji Finansowej 2001*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 2001.
14. Mitnick K., Simon W., *Łamałem ludzi, nie hasła. Sztuka podstępu*, Helion, Gliwice 2002.
15. PN-I-02000:2002. *Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia.*
16. PN-ISO/IEC 17799/2007. *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.*
17. PN-ISO/IEC 20000–1:2014–01. *Technika informatyczna. Zarządzanie usługami. Część 1: Wymagania dla systemu zarządzania usługami.*
18. PN-ISO/IEC 20000–2:2007. *Technika informatyczna. Zarządzanie usługami. Część 2: Reguły postępowania.*
19. PN-ISO/IEC 2382–8:2001. *Technika informatyczna. Terminologia. Część 8: Bezpieczeństwo.*
20. PN-ISO/IEC 24762:2010. *Technika informatyczna. Techniki bezpieczeństwa. Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.*
21. PN-ISO/IEC 27001:2007. *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*
22. PN-ISO/IEC 27005:2014–01. *Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji.*
23. Raport Techniczny ISO/IEC TR 13335–3/1998. *Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Techniki zarządzania bezpieczeństwem systemów informatycznych.*
24. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 5 czerwca 2014 r. w sprawie zasad potwierdzania, przedłużania ważności, unieważniania oraz wykorzystania profilu zaufanego elektronicznej platformy usług administracji publicznej (Dz.U. z 2014, poz. 778 ze zm.).
25. Rozporządzenie Ministra Finansów z dnia 26 kwietnia 2012 r. zmieniające rozporządzenie w sprawie określenia rodzajów deklaracji, które mogą być składane za pomocą środków komunikacji elektronicznej (Dz.U. z 2012 r., poz. 474 ze zm.).
26. Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 2 listopada 2007 r. w sprawie systemów teleinformatycznych stosowanych w jednostkach organizacyjnych pomocy społecznej (Dz.U. z 2007 r. nr 216, poz. 1609 ze zm.).

27. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., nr 100, poz. 1024 ze zm.).
28. Rozporządzenie Ministra Spraw Wewnętrznych z dnia 25 kwietnia 2014 r. zmieniające rozporządzenie w sprawie trybu dostępu i wzoru upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz wykorzystywania danych (Dz.U. z 2014 r., poz. 558 ze zm.).
29. Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych (Dz.U. z 2004 r. nr 100, poz. 1023 ze zm.).
30. Rozporządzenie Ministra Sprawiedliwości z dnia 29 grudnia 2011 r. w sprawie trybu zakładania konta w systemie teleinformatycznym, sposobu korzystania z systemu teleinformatycznego i podejmowania w nim czynności związanych z zawiązaniem spółki z ograniczoną odpowiedzialnością przy wykorzystaniu wzorca umowy oraz wymagań dotyczących podpisu elektronicznego (Dz.U. z 2011 r. nr 297, poz. 1762 ze zm.).
31. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. z 1999 r. nr 18, poz. 162 ze zm.).
32. Rozporządzenie Prezesa Rady Ministrów z dnia 8 maja 2014 r. zmieniające rozporządzenie w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2014 r., poz. 590 ze zm.).
33. Rozporządzenie 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 (Dz.U. z 2012 r., poz. 526 ze zm.).
34. Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty i warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. z 2002 r. nr 128, poz. 1094 ze zm.).
35. Szczepankiewicz E.I., *Jak chronić dane finansowe w środowisku informatycznym rachunkowości*, „Biuletyn Rachunkowości i Finansów" 2007, nr 8(32).

36. Szczepankiewicz E.I., *Wybrane procedury kontroli wewnętrznej w środowisku informatycznym rachunkowości*, w: *Rachunkowość w teorii i praktyce*, t. I, *Rachunkowość finansowa*, red. W. Gabrusewicz, Wydawnictwo Akademii Ekonomicznej w Poznaniu, Poznań 2007.
37. Szczepankiewicz E.I., *Analiza ryzyka jako element systemu kontroli w firmie*, „Biuletyn Rachunkowości" 2008, nr 14.
38. Szczepankiewicz E.I., *Jakie są zasady opracowywania procedur kontrolnych w firmie*, „Biuletyn Rachunkowości" 2008, nr 12(60).
39. Szczepankiewicz E.I., *Audyt sprawozdań finansowych w środowisku informatycznym*, w: *Audyt sprawozdań finansowych*, red. W. Gabrusewicz, PWE, Warszawa 2010, s. 198.
40. Szczepankiewicz E.I., *Audyt sprawozdań finansowych w środowisku informatycznym*, w: *Audyt sprawozdań finansowych. Teoria i praktyka*, red. W. Gabrusewicz, PWE, Warszawa 2014.
41. Szczepankiewicz E.I., *Audyt kontroli wewnętrznej rachunkowości w środowisku informatycznym*, Difin, Warszawa 2016.
42. Szczepankiewicz E.I., *Kontrola zarządcza w jednostkach samorządu terytorialnego. Doskonalenie procedur kontroli zarządczej w środowisku informatycznym rachunkowości*, Wydawnictwo Naukowe CONTACT, Poznań 2016.
43. Szczepankiewicz E.I., *Zasady i procedury kontroli zarządczej w obszarze systemów informatycznych rachunkowości w jednostkach sektora finansów publicznych*, Wydawnictwo Naukowe CONTACT, Poznań 2016.
44. Szczepankiewicz E.I., Dudek M., *Rozwój technologii informatycznych a zagrożenia i zarządzanie bezpieczeństwem informacji w przedsiębiorstwach*, w: *Logistyka – Komunikacja – Bezpieczeństwo, Wybrane problemy*, red. M. Grzybowski, J. Tomaszewski, Wydawnictwo Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni, Gdynia 2009.
45. *The 2011 Cloud Dividend report*, http://uk.emc.com/microsites/2010/cloud-dividend/index.htm (dostęp 12.02.2016).
46. Ustawa z 6 czerwca 1997 r. Kodeks karny (Dz.U. z 1997 r. nr 55, poz. 553 z późn. zm.).
47. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2013 r., poz. 235 ze zm.).
48. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r. nr 144, poz. 1204 ze zm.).
49. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2013 r., poz. 262 ze zm.).
50. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 1997 r. nr 114, poz. 740 ze zm.).

51. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2001 r. nr 128, poz. 1402 ze zm.).
52. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (tj. Dz.U. z 2016 r., poz. 1870 ze zm.).
53. Ustawa z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa oraz o zmianie niektórych ustaw (Dz.U. z 2013 r., poz. 194 ze zm.).
54. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. nr 101, poz. 926 ze zm.).
55. Wójcik J.W., *Przestępstwa komputerowe*, cz. 1, *Fenomen cywilizacji*, CIM, Warszawa 1999.
56. Wójcik J.W., *Przestępstwa komputerowe*, cz. 2, *Techniki zapobiegania*, CIM, Warszawa 1999.

Threats to Accounting IT Resources at the Age of Information Technology Transformation in the Public Finance Entities

Summary

An important aspect of the appropriate level of efficiency and quality of operation in the entities of public finance is to ensure the continuity of IT operation and security of IT resources. The use of IT systems and teleinformation technology in these entities is connected with numerous threats related to the IT environment. The article discusses the most important threats with regard to a traditional model of IT resources management in entities and a new model of cloud computing. It mentions the problem of threats and conclusions from the research in the context of technological transformations as well as imperfectness of management control systems, which do not always keep up with these changes. The research method used in the study is the review of the literature, legal regulations, management control standards, internal audit standards, ISO norms as well as drawing conclusions.

Keywords: accounting, IT system, threats, IT resources security, risk management, management control system, cloud computing

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 31–46

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

Grażyna Voss
Wydział Zarządzania
Uniwersytet Technologiczno-Przyrodniczy w Bydgoszczy

Rachunkowość w procesie cyfryzacji – obszary ryzyka

Streszczenie

W artykule zawarte zostały podstawowe założenia związane z wdrożeniem procesów cyfryzacji w rachunkowości i realizacją wytycznych nałożonych na kraje członkowskie UE, a wynikających z Dyrektywy Parlamentu Europejskiego i Rady 2012/17/UE z dnia 13 czerwca 2012 r. zmieniającej dyrektywę Rady 89/666/EWG i dyrektywy Parlamentu Europejskiego i Rady 2005/56/WE i 2009/101/WE w zakresie integracji rejestrów centralnych, rejestrów handlowych i rejestrów spółek. Opis nowych rozwiązań związanych z eksportem danych finansowych i sporządzaniem e-wniosków został opracowany na podstawie zmian wprowadzonych w polskich regulacjach prawnych z uwzględnieniem terminów ich wdrożenia. Ponadto wskazano korzyści i zagrożenia wynikające z funkcjonowania podmiotów gospodarczych w cyberprzestrzeni.

Słowa kluczowe: Jednolity Plik Kontrolny, cyfryzacja, informacja podatkowa
Kody klasyfikacji JEL: M41, M48

1. Wprowadzenie

Rozwój technologii informacyjno-komunikacyjnych wprowadził liczne zmiany w życiu gospodarczym i społecznym oraz sposobie funkcjonowania jednostek w XXI w.[1]. Doprowadził on do funkcjonowania podmiotów gospodarczych i interesariuszy w wirtualnej przestrzeni[2] (cyberprzestrzeni), w której komunikacja odbywa się między komputerami połączonymi siecią. Dla użytkowników funkcjonowanie w sieci, oprócz licznych korzyści[3], generuje również różnego rodzaju zagrożenia i nowe obszary ryzyka. Są one związane z naruszeniem bezpieczeństwa informacji, systemów informacyjnych, modyfikowaniem wcześniej wygenerowanych informacji czy w końcu z możliwością dostępu do informacji wykorzystywanych w analizie i procesie decyzyjnym. Do najczęściej wymienianych przyczyn zagrożeń zaliczyć można działania przypadkowe oraz świadome i celowe, takie jak oszustwa i szpiegostwo komputerowe czy nawet hakerstwo. Zapewnienie zabezpieczeń stanowi istotne wyzwanie dla wszystkich użytkowników, zarówno instytucjonalnych, jak i indywidualnych. Wykorzystanie współczesnych technologii stało się nieodzownym elementem funkcjonowania podmiotów na rynku; związane jest z szybkim dostępem i pozyskiwaniem informacji[4] oraz kosztami związanymi z wdrożeniem technologii i stosownych zabezpieczeń.

Celem artykułu jest zaprezentowanie zmian wynikających z wdrożenia procesu cyfryzacji w rachunkowości oraz korzyści i zagrożeń wynikających z tego procesu. Do realizacji celu wykorzystano analizę uregulowań prawnych, w tym planowane zmiany w przepisach wchodzące w życie od 2018 r. oraz dane statystyczne z Departamentu Strategii i Deregulacji Ministerstwa Sprawiedliwości.

---

[1] R.W. Scapens, M. Ezzamel, J. Burns, G. Baldvinsdottir, *The Future Direction of UK Management Accounting Practice*, Elsevier/CIMA Publications, London, 2003

[2] G. Siegel, J.E. Sorensen, *Counting More, Counting Less: The New Role of Management Accountants*, „Transformations in the Management Accounting Profession" 1999, vol. 3, Institute of Management Accountants.

[3] A. Jabłoński, M. Kawczyńska, Ż. Pietrzak, T. Wnuk-Pel, *Oczekiwania wpływu implementacji zintegrowanego systemu informatycznego na jakość informacji – studium przypadku*, „Zeszyty Teoretyczne Rachunkowości" 2016, t. 89(145), s. 56.

[4] E.J. Umble, R.R. Haft, M. Umble, *Enteprise Resource Planning: Implementation Procedures and Critical Success Factors*, „European Journal of Operational Research" 2003, 146(2), s. 242–254.

2. Pojęcie i istota cyberprzestrzeni

Nieustanne zmiany wywołane postępem technologicznym, codziennie kreują nowe możliwości i wyzwania, a techniki komputerowe stają się powszechnie wykorzystywane i stosowane we wszystkich obszarach działalności człowieka. Przejawem tych działań jest ogólnoświatowa wymiana informacji, e-bankowość, e-usługi, e-handel, podpis elektroniczny, czyli wirtualizacja rzeczywistości i cyfryzacja życia współczesnego społeczeństwa. Dostarczanie i przetwarzanie ogromnych ilości informacji o osobach i ich działalności stało się tak powszechne, że trudno sobie wyobrazić świat bez Internetu. Ponadto dla wielu osób wykładnikiem statusu społecznego stała się liczba osób zaproszonych do grona znajomych, dla innych wirtualne zakupy czy też dostęp do sieciowej gry komputerowej. Działania te zaowocowały powstaniem cyberprzestrzeni, której początki zaczynają się ponad 30 lat temu. Z uwagi na rosnące znaczenie funkcjonowania i wykorzystania sieci w życiu gospodarczym, konieczne stało się rozpoznanie nowego cyfrowego środowiska, które doprowadziło do podejmowania określonych działań, takich jak zawieranie umów cywilnoprawnych, wykonywanie prac zawodowych, czynności administracyjnych i w końcu do popełniania czynów prawnie niedozwolonych czy przestępstw. Cyberprzestrzeń została zdefiniowana jako: „przestrzeń wirtualna, w której odbywa się komunikacja między komputerami połączonymi siecią internetową”[5]. Jest ona również definiowana w różnych regulacjach prawnych wielu państw świata. Proces informatyzacji został również wprowadzony do polskiego porządku prawnego i określa go Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne[6]. Wraz z rozwojem cyberprzestrzeni wzrasta ryzyko występowania zagrożeń. W Polsce powstał Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016 i w połowie 2013 r. opublikowano dokument pod nazwą Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej[7]. Podsumowując, można zauważyć, że cyberprzestrzeń stała się nieodzownym elementem funkcjonowania współczesnego świata, swoistego rodzaju równoległym środowiskiem, będącym nowym wymiarem ludzkich działań, dla których zapewnienie odpowiedniego poziomu ochrony jest niezbędne

[5] http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915, dostęp 10.11.2016.

[6] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne, Dz.U. z 2016 r., poz. 352.

[7] https://mac.gov.pl/files/nask_rekomendacja.pdf, dostęp 11.11.2016.

ze względu na różnorodność konotacji prawnych. Jednak szacowanie kosztów związanych z wdrożeniem, utrzymaniem i rozwojem systemu ochrony cyberprzestrzeni, zarówno na szczeblu krajowym, jak i poszczególnych interesariuszy, nie jest możliwe ze względu na dynamikę zmian i nowe zagrożenia.

3. Cyberprzestrzeń w rachunkowości

Wykorzystanie informatycznych systemów finansowo-księgowych pozwala na dostarczanie użytkownikom wewnętrznym i zewnętrznym informacji z dowolną częstotliwością i o wybranym poziomie szczegółowości, co potwierdzają badania przeprowadzone przez różnych autorów[8]. Informacje wprowadzone do systemu pozwalają na ich wieloobszarowe przetwarzanie i opracowywanie raportów; jednocześnie nie wymaga to dodatkowego nakładu pracy[9]. W art. 20 ustawy o rachunkowości[10] zostały określone zasady prowadzenia ksiąg rachunkowych przy użyciu komputera. Zasady te zakładają automatyczne wprowadzanie zapisów za pośrednictwem urządzeń łączności i informatycznych nośników danych przy zapewnieniu, że podczas rejestrowania tych zapisów zostaną spełnione określone warunki:

- zapisy uzyskają trwale czytelną postać, zgodną z treścią odpowiednich dowodów księgowych,
- możliwe jest stwierdzenie źródła ich pochodzenia oraz ustalenie osoby odpowiedzialnej za ich wprowadzenie,
- stosowana procedura zapewnia sprawdzenie poprawności przetworzenia odnośnych danych oraz kompletności i identyczności zapisów,
- dane źródłowe w miejscu ich powstania są odpowiednio chronione, w sposób zapewniający ich niezmienność, przez okres wymagany do przechowywania danego rodzaju dowodów księgowych.

Wymagania określone przez ustawodawcę mają charakter ogólny i pozostawiają dużą swobodę działania w zakresie wyboru i wdrożenia oprogramowania

[8] W. Zalewski, *Analiza systemów informatycznych wspomagających zarządzanie produkcji w wybranych przedsiębiorstwach*, „Economy and Management" 2011, 4; zob. J. Rut, E. Kulińska, *Zintegrowany system informatyczny w przedsiębiorstwie produkcyjnym*, „Logistyka" 2013, 1.

[9] G. Voss, P. Prewysz-Kwinto, *Zintegrowane systemy ewidencyjne*, w: *Przyszłość rachunkowości i sprawozdawczości – założenia, zasady, definicje. Kierunki zmian prawa bilansowego w Polsce*, red. Z. Luty, A. Łakomiak, A. Mazur, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2013, s. 149.

[10] Ustawa z dnia 29 września 1994 r. o rachunkowości, Dz.U. z 2016 r., poz. 615.

obsługującego system finansowo-księgowy oraz opracowania szczegółowych zasad prowadzenia ksiąg rachunkowych.

Zmiany w zakresie cyfryzacji w rachunkowości nakładają jednak na jednostki gospodarcze dodatkowe obowiązki w zakresie przygotowywania i przesyłania danych finansowo-księgowych w wersji elektronicznej. Z dniem 1 lipca 2016 r. weszły w życie nowe przepisy Ordynacji podatkowej, wprowadzającej reguły udostępniania organom podatkowym informacji wynikających z ksiąg rachunkowych i dowodów księgowych, nazwane Jednolitym Plikiem Kontrolnym (JPK). Nowe obowiązki podatników zakładają udostępnianie organom podatkowym w postaci elektronicznej całości lub części ksiąg rachunkowych oraz dowodów księgowych w wersji elektronicznej, przy jednoczesnym zapewnieniu bezpieczeństwa i wiarygodności, a także ochrony przed dostępem osób nieuprawnionych. Przepisy te wprowadzają przekazywanie danych w postaci logicznej struktury, która możliwa jest do uzyskania przy powszechnie stosowanych programach komputerowych. Organizacja Współpracy Gospodarczej i Rozwoju (OECD) w 2010 r. zdefiniowała JPK jako zbiór danych, tworzonych z systemów informatycznych podmiotu gospodarczego (bezpośredni eksport danych), zawierający informacje o operacjach gospodarczych za dowolnie wybrany okres oraz mający układ i format (XML) umożliwiający jego łatwe przetwarzanie[11]. W polskich przepisach nie został wskazany format XML, pozwalając jednostkom na przedstawienie JPK w formie logicznej struktury i pozostawiając do wyboru możliwość wdrożenia innych formatów, np. UBL lub XBRL[12].

Przesyłanie JPK może być realizowane jako przekazanie ksiąg podatkowych i dokumentów na żądanie organów kontroli (art. 193a Op.) lub bez wezwania organu podatkowego (art. 109 ust. 3 ustawy o podatku od towarów i usług).

Ważnym elementem w zakresie elektronicznego przesyłania danych jest okres wprowadzenia obowiązku. W przypadku przesyłania raportów na żądanie organów podatkowych należy wyodrębnić dwa terminy:

- lipiec 2016 dla dużych podmiotów,
- lipiec 2018 dla mikro, małych i średnich podmiotów.

Dla określenia wielkości podmiotów ustawodawca przedstawił kryteria podziału: wielkość zatrudnienia, roczny obrót i sumę aktywów. Dla dużych podmiotów kryteria te przedstawiają się następująco: zatrudnienie 250 i więcej pracowników lub

[11] J. Oleśniewicz, *JPK – wstęp do cyfryzacji rachunkowości i rewizji finansowej*, „Rachunkowość" 2016, 8, s. 18.

[12] K.P. Ramin, C.A., Reiman, *IFRS and XBRL*, WILEY, A.J. Willey &Sons, Publication, London 2013, s. 458–469.

obrót powyżej 50 mln euro i aktywa powyżej 43 mln euro. Wielkości te dla średnich i małych podmiotów przedstawiają się następująco: zatrudnienie poniżej 250 pracowników oraz obrót mniejszy lub równy 50 mln euro lub aktywa mniejsze lub równe 43 mln euro. Do mikropodmiotów zaliczyć można te jednostki, których wielkość zatrudnienia jest mniejsza niż 10 pracowników oraz obroty są mniejsze lub równe 2 mln euro lub aktywa są mniejsze lub równe 2 mln euro.

Elektroniczne raportowanie miesięczne na cele podatku VAT (bez wezwania organu podatkowego) są obowiązkowe dla dużych jednostek od lipca 2016, małe i średnie podmioty obowiązek takiego raportowania mają od stycznia 2017, a mikropodmioty – od stycznia 2018 r.

Podstawowym celem JPK jest eliminowanie przestępstw i nieprawidłowości w naliczaniu podatków. W swoim założeniu działania te mają na celu realizację czynności sprawdzających, dzięki czemu kontrola u podatnika nie będzie konieczna.

Kolejna propozycja zmian w zakresie elektronicznego przekazywania informacji to e-wnioski, składane do Krajowego Rejestru Sądowego. Zmiany wprowadzone z dniem 1 kwietnia 2016 r. pozwolą podatnikom na elektroniczne składanie wszystkich e-wniosków do KRS, należy jednak pamiętać, że ze względów bezpieczeństwa wnioski muszą być podpisane elektronicznie (potwierdzonym profilem zaufania ePUAP bądź opatrzone bezpiecznym e-podpisem bądź podpisem elektronicznym). Docelowo wnioski papierowe zostaną całkowicie wyparte przez elektroniczne. Szczegółowe przepisy w zakresie stosowania składania wniosków i podpisów elektronicznych reguluje Kodeks postępowania cywilnego[13]. Również sąd będzie udzielał odpowiedzi drogą elektroniczną za pośrednictwem systemu teleinformacyjnego, obsługującego postępowanie rejestrowe. Wprowadzone zmiany wymuszają regulacje prawa Unii Europejskiej zawarte w Dyrektywie Parlamentu Europejskiego i Rady 2012/17/UE z dnia 13 czerwca 2012 r. zmieniającej dyrektywę Rady 89/666/EWG i dyrektywy Parlamentu Europejskiego i Rady 2005/56/WE i 2009/101/WE w zakresie integracji rejestrów centralnych, rejestrów handlowych i rejestrów spółek (określanej jako dyrektywa BRIS). Zobowiązuje ona państwa członkowskie do wymiany danych dotyczących spółek oraz dostępu do aktualnych i wiarygodnych informacji o spółkach. Konieczność implementacji dyrektywy BRIS powoduje m.in., że Ministerstwo Sprawiedliwości pracuje nad projektem ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw.

[13] Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego, Dz.U. z 2016 r., poz. 1358.

Kolejne zmiany dotyczące funkcjonowania KRS weszły w życie 1 czerwca 2017 r. Dotyczą wprowadzenia obowiązku składania wszystkich wniosków do rejestru przedsiębiorców KRS oraz dokumentów stanowiących podstawę wpisu lub podlegających dołączeniu do akt rejestrowych drogą elektroniczną. Wyjątek będą stanowiły podmioty, które podlegają wpisowi wyłącznie do rejestru stowarzyszeń i innych organizacji społecznych i zawodowych, fundacji, samodzielnych publicznych zakładów opieki zdrowotnej. Będą one mogły skorzystać z e-wniosku, ale nie będą miały takiego obowiązku.

Ponadto zmiany dotyczyć będą również:

- stworzenia przez Krajową Radę Notarialną elektronicznego repozytorium wypisów aktów i protokołów notarialnych, umożliwiającego składanie przez strony wszystkich dokumentów dołączonych do wniosku w formie elektronicznej,
- umożliwienia stronom i sądowi wymiany korespondencji z wykorzystaniem systemu bez konieczności ponownego wypełniania formularza (wezwania brakowe, uzupełnienia braków wniosku) w ramach prowadzonego postępowania,
- umożliwienia sądowi rejestrowemu wydawania w toku postępowania zarządzeń o charakterze technicznym w formie elektronicznej,
- połączenia systemu teleinformatycznego, w którym składane będą wnioski z systemem wpisów, co umożliwi automatyczne sporządzenie projektu postanowienia bez konieczności ręcznego wpisywania danych przez pracowników administracyjnych sądu,
- doręczania orzeczeń i pism sądowych za pośrednictwem systemu teleinformatycznego,
- prowadzenia akt rejestrowych podmiotów wpisanych do rejestru przedsiębiorców KRS w formie elektronicznej i ich udostępnianie w czytelni akt,
- zapewnienia digitalizacji pism wpływających i wysyłanych w formie papierowej do i z akt rejestrowych prowadzonych w formie elektronicznej,
- umożliwienia złożenia środków zaskarżenia z wykorzystaniem systemu teleinformatycznego.

Z dniem 8 czerwca 2017 r. rozpoczęła się integracja Krajowego Rejestru Sądowego z systemem integracji rejestrów (BRIS).

Natomiast kolejne zmiany planowane są na wrzesień 2018 r. i dotyczą:

- stworzenia ogólnodostępnego portalu internetowego, udostępnienia dokumentów sądowych wytworzonych w systemie informatycznym KRS i dokumentów złożonych przez stronę; dostęp do tych informacji będzie nieograniczony; każdy

będzie mógł do nich sięgnąć; obecnie, aby zapoznać się z aktami rejestrowymi, trzeba złożyć zapotrzebowanie na akta z kilkudniowym wyprzedzeniem;
- wprowadzenia usługi newslettera, polegającej na generowaniu powiadomień o doręczanych stronie dokumentach sądowych wnioskodawca otrzyma niezwłocznie powiadomienie o umieszczeniu na jego koncie dokumentów sądowych w jego sprawie;
- **wprowadzenia obowiązku składania sprawozdań finansowych w formie elektronicznej w odpowiednim formacie danych, ułatwiającym późniejsze wykorzystanie tych danych**;
- rezygnacji z publikacji wpisów w Monitorze Sądowym i Gospodarczym;
- udostępnienia w Internecie pełnych danych o podmiocie; aktualnie poprzez wyszukiwarkę KRS każdy ma dostęp do aktualnych danych o podmiocie; natomiast uzyskanie pełnych danych (aktualnych i historycznych) wymaga uzyskania odpisu pełnego z KRS;
- automatycznego przekazywania danych zawartych w rejestrze zainteresowanym instytucjom.

Zaprezentowane zmiany zostały opracowane na podstawie projektu założeń ustawy o zmianie ustawy o KRS oraz niektórych innych ustaw (wersja z 23 lutego 2016 r.). Zakres zmian spowodowanych cyfryzacją jest stosunkowo obszerny. Warto jednak zauważyć, że okres przygotowania się do zmian został wydłużony przede wszystkim dla mikropodmiotów, których mobilność ze względu na niewielką liczbę pracowników może być ograniczona, jak również ograniczone mogą być możliwości finansowe wymagane do dostosowania systemu finansowo-księgowego oraz innych programów użytkowych.

4. Korzyści i zagrożenia związane z wdrożeniem procesu cyfryzacji

Zmiana systemów informatycznych w firmach dokonywana jest z różną częstotliwością, w zależności od indywidualnych potrzeb i możliwości jednostki, jednak za każdym razem związane jest to z dużym obciążeniem dla pracowników. Coraz częściej zarówno duże, jak i małe podmioty decydują się na wdrożenie zawansowanych, zintegrowanych systemów informatycznych. Z jednej strony usprawniają one pracę i umożliwiają otrzymanie potrzebnych informacji znacznie szybciej, z drugiej ich wdrożenie wiąże się z dużym wysiłkiem pracowników i znacznymi kosztami. Ponadto

wdrożenie nowych systemów informatycznych pozwoli jednostkom na sporządzanie JPK oraz eksport danych dotyczących sprawozdań finansowych, ksiąg i rejestrów.

Rachunkowość jest uniwersalnym i elastycznym systemem ewidencyjno-kontrolnym, dzięki czemu wykorzystywana jest we wszystkich podmiotach gospodarczych bez względu na ich wielkość i charakter prowadzonej działalności. W tym miejscu można również zauważyć, że zintegrowane systemy ewidencyjne są uniwersalne i wychodzą naprzeciw indywidualnym oczekiwaniom poszczególnych użytkowników. Ich uniwersalność pozwoli użytkownikom na dostosowanie wykorzystywanego oprogramowania do realizacji obowiązków prawnych związanych z elektronicznym przekazywaniem wniosków, deklaracji, ksiąg podatkowych, dokumentów księgowych czy też docelowo sprawozdań finansowych. Ten charakter unikatowych rozwiązań wdrażanych w jednostkach gospodarczych ma wiele zalet, ale ze względu na indywidualne podejście do użytkownika wymusza każdorazowo na pracownikach działów finansowo-księgowych przejście procesu wdrożenia, w celu zagwarantowania prawidłowej obsługi programu. W takiej sytuacji trudno mówić o harmonizacji i standaryzacji rozwiązań we wszystkich aspektach księgowych. Ujednolicenie zasad funkcjonowania zintegrowanych systemów zostanie ograniczone jedynie w aspekcie rachunkowości normatywnej, dla której generowanie raportów uwarunkowane jest wymogami ustawodawcy, np. w zakresie sporządzania rejestrów VAT, sprawozdań na potrzeby urzędów skarbowych czy GUS.

W związku z możliwościami wykorzystania zintegrowanych systemów informatycznych nowego znaczenia nabiera funkcja informacyjna rachunkowości. Dzięki „nieograniczonym" możliwościom generowania raportów i zestawień jednostka jest w stanie w krótkim przedziale czasu uzyskać dowolny raport, na podstawie którego kierownictwo jednostki będzie mogło podjąć określone decyzje. Zintegrowane systemy informatyczne dzięki realizowanym funkcjom pozwalają na osiągnięcie określonych korzyści przez jednostkę, ale wdrożenie tych systemów może wiązać się z określonymi utrudnieniami.

Korzyści wynikające z wdrożenia zintegrowanych systemów w działach finansowo-księgowych pozwalają na[14]:

- skrócenie czasu zamknięć miesięcznych i rocznych oraz zwiększenie dokładności sporządzanych raportów,
- opracowanie wybranych raportów i zestawień w różnym ujęciu,

[14] G. Voss, P. Prewysz-Kwinto, *Zintegrowane*…, op.cit. s. 157.

- ograniczenie ryzyka niezgodności dzięki wykorzystaniu międzynarodowych i krajowych standardów rachunkowości,
- przeprowadzenie pogłębionych analiz w krótkim przedziale czasu,
- gromadzenie i przetwarzanie dowolnych informacji.

Wdrożenie nowoczesnych rozwiązań wiąże się również z utrudnieniami, do których zalicza się[15]:

- czasochłonność wyboru partnera wdrożeniowego,
- czasochłonność dopracowania, wdrożenia, testowania systemu,
- dobór pracowników będących kluczowymi użytkownikami, odznaczającymi się szerszym poglądem na problemy funkcjonowania jednostki gospodarczej,
- zachowanie systematycznej i chronologicznej ewidencji księgowej, poprzez wykorzystanie wielokrotnego zapisu na dyskach bez zachowania śladu wprowadzania zmian,
- ograniczenie zatrudnienia w działach księgowych, dobór wykwalifikowanej kadry pracowniczej,
- możliwość popełnienia błędów przez użytkowników, ze względu na złożoność systemu (tzw. czynnik ludzki).

Jednostki gospodarcze przystępujące do wdrożenia systemu muszą liczyć się również z kosztami takiego wdrożenia oraz kosztami związanymi z obsługą powdrożeniową, jednak stosowanie tych systemów w XXI w. staje się powszechną praktyką w zakresie obsługi firm. Korzyści wynikające z cyfryzacji w rachunkowości odnoszone są również do instytucji takich, jak organy podatkowe czy KRS. Z jednej strony pozwolą na lepszą kontrolę i nadzór mający na celu ukrócenie przestępstw i nieprawidłowości, z drugiej strony będą wymagały od tych instytucji dostosowania odpowiednich nośników do gromadzenia, analizowania i przechowywania danych uzyskanych od interesariuszy.

Mając na uwadze powyższe korzyści, należy zwrócić uwagę, że ujawnianie informacji w JPK czy docelowo składanie sprawozdań w formie elektronicznej stanowi jedynie formę przekazania informacji. Czy cyfryzacja poprawi rzetelność prowadzenia ksiąg rachunkowych i wiarygodność sprawozdań finansowych? Doświadczenia ostatnich lat ukazują liczne niedociągnięcia w tym zakresie. Prawomocne wyroki wydane na podstawie Ustawy z dnia 29 września 1994 r. o rachunkowości związane z nieprowadzeniem ksiąg rachunkowych czy też nierzetelnym ich prowadzeniem,

[15] Ibidem, s. 158.

niesporządzaniem sprawozdań finansowych bądź prezentowaniem w nich nierzetelnych danych przedstawiono w tabeli 1.

Tabela 1. Prawomocne skazania osób dorosłych – zgodnie z art. 77 Ustawy z dnia 29 września 1994 r. o rachunkowości

Lata	Ogółem liczba wyroków	Nieprowadzenie ksiąg rachunkowych, prowadzenie ich wbrew przepisom ustawy lub podawanie w tych księgach nierzetelnych danych (art. 77 ust. 1)	Niesporządzenie sprawozdań finansowych i innych, sporządzenie ich niezgodnie z przepisami ustawy lub zawarcie w tych sprawozdaniach nierzetelnych danych (art. 77 ust. 2)
2001	42	3	19
2002	24	1	14
2003	55	11	16
2004	141	36	36
2005	169	47	22
2006	219	58	45
2007	234	41	38
2008	417	56	66
2009	416	53	67
2010	455	51	54
2011	446	42	55
2012	549	54	85
2013	802	66	128
2014	701	42	125
RAZEM	4670	561	770

Źródło: opracowanie własne na podstawie danych uzyskanych z Wydziału Statystycznej Informacji Zarządczej Departamentu Strategii i Deregulacji Ministerstwa Sprawiedliwości z 23 września 2013 r. i 26 sierpnia 2015 r.

Z danych zaprezentowanych w tabeli 1 nie można określić, jaki charakter działalności prowadziły jednostki gospodarcze, w których osoby odpowiedzialne za rzetelność ksiąg rachunkowych i sporządzanie sprawozdań zostały skazane prawomocnymi wyrokami. Nie można też określić formy organizacyjnoprawnej ani wielkości jednostki[16]. Prawomocne wyroki w zakresie rzetelności ksiąg rachunkowych i wiarygodności sprawozdań finansowych zapadały nie tylko na podstawie

[16] G. Voss, *Kształtowanie norm etycznych a odpowiedzialność zawodowa księgowych*, Wydawnictwo Uczelniane Uniwersytetu Technologiczno-Przyrodniczego w Bydgoszczy, Bydgoszcz 2016, s. 115.

Ustawy o rachunkowości, lecz także na podstawie Kodeksu karnego i Kodeksu karnego skarbowego, co zaprezentowano w tabeli 2.

Tabela 2. Nieprowadzenie, wadliwe lub nierzetelne prowadzenie ksiąg rachunkowych – wyroki sądowe wydane na podstawie Kodeksu karnego, Ustawy o rachunkowości i Kodeksu karnego skarbowego w latach 2001–2014

Lata	Akty prawne			Łączna liczba wyroków
	Kodeks karny	Ustawa o rachunkowości	Kodeks karny skarbowy	
2001	74	22	135	231
2002	90	15	154	259
2003	108	27	217	352
2004	180	72	305	557
2005	196	69	309	574
2006	189	103	258	550
2007	91	79	202	372
2008	153	122	224	499
2009	176	120	222	518
2010	263	105	280	648
2011	210	97	269	576
2012	190	139	234	563
2013	152	194	218	564
2014	193	167	219	579
RAZEM	2265	1331	3246	6842

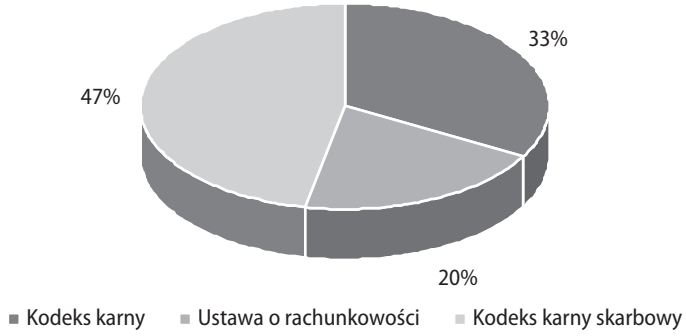
Źródło: jak pod tab. 1.

Rozpatrując łącznie liczbę wyroków związanych z nieprawidłowościami w zakresie prowadzenia ksiąg rachunkowych i sporządzania sprawozdań finansowych, można zauważyć, że w ciągu 14 lat wydano blisko 7000 wyroków. Nie odzwierciedla to skali badanego zjawiska, a jedynie wskazuje, ile osób naruszających przepisy prawne zostało pociągniętych do odpowiedzialności.

Analizując łączną liczbę prawomocnych wyroków w latach 2001–2014 z tytułu nieprowadzenia lub nierzetelnego prowadzenia ksiąg rachunkowych, można zauważyć, że prawie połowa (47%) wyroków została wydana na podstawie Kodeksu karnego skarbowego. Zaledwie co piąty wyrok (20%) związany z nieprowadzeniem

lub nierzetelnym prowadzeniem ksiąg rachunkowych zapadł na podstawie art. 77 ustawy o rachunkowości (rysunek 1).

Rysunek 1. Struktura najczęściej wykorzystywanych aktów prawnych w celu stwierdzenia nieprawidłowości w zakresie prowadzenia ksiąg rachunkowych w latach 2001–2014



Źródło: opracowanie własne.

Wynika to z wielofunkcyjności informacji księgowych zawartych w księgach rachunkowych oraz możliwości wykorzystania zawartych w nich informacji w różnych obszarach, m.in. podatkowych, rozliczeniowych, sprawozdawczych, analitycznych i innych.

Na podstawie zaprezentowanych danych można zauważyć iż w latach 2001–2014, pomimo stosowanych powszechnie programów finansowo-księgowych, miały miejsce nieprawidłowości w zakresie rzetelności ksiąg rachunkowych i sprawozdawczości. Ponadto wraz z upływem czasu i postępem technologicznym liczba prawomocnych wyroków nie uległa zmniejszeniu. Czy w związku z tym cyberprzestrzeń i cyfryzacja w rachunkowości wpłynie na poprawę jakości informacji finansowych?

5. Podsumowanie

Funkcjonowanie podmiotów gospodarczych w cyberprzestrzeni jest naturalnym procesem rozwoju gospodarczego. Cyfryzacja rachunkowości wynika z dyrektyw Unii Europejskiej i wdrożona została krajowymi regulacjami prawnymi. Jednostki gospodarcze, w zależności od wielkości podmiotu, zmuszone są do dostosowania swojego systemu finansowo-księgowego i wprowadzenia zmian w określonym przez

ustawodawcę terminie. Cyberprzestrzeń i cyfryzacja stwarza nowe możliwości rozwoju, ale również jest źródłem dynamicznie zmieniających się zagrożeń. Stosowanie programów finansowo-księgowych pozwala na generowanie dokumentów księgowych, tworzenie w dowolnych układach raportów, zestawień i sprawozdań finansowych z możliwością bezpośredniego eksportu tych danych. Takie rozwiązania usprawniają pracę i skracają czas poświęcony na jej wykonanie, stwarzają nowe możliwości rozwoju kontroli wewnętrznej. Chociaż elektroniczny przekaz danych wymaga dodatkowych zabezpieczeń, to jednak jako narzędzie pracy nie zabezpieczy i nie wyeliminuje naruszeń związanych z nierzetelnym prowadzeniem ksiąg rachunkowych bądź generowaniem sprawozdań finansowych zawierających niewiarygodne informacje finansowe. Złożoność przepisów, czynnik ludzki lub świadome działanie mające na celu generowanie informacji finansowych z naruszeniem przepisów prawnych nie zostaną wyeliminowane poprzez stosowanie nowych narzędzi i rozwiązań technologicznych. Bez wątpienia istotną rolę w procesie cyfryzacji rachunkowości będzie odgrywało profesjonalne przygotowanie zawodowe księgowych, realizowane w ramach rozwoju zawodowego i procesu samokształcenia, oraz przestrzeganie norm etyki zawodowej.

Bibliografia

1. Dyrektywa Parlamentu Europejskiego i Rady 2012/17/UE z dnia 13 czerwca 2012 r. zmieniająca dyrektywę Rady 89/666/EWG i dyrektywy Parlamentu Europejskiego i Rady 2005/56/WE i 2009/101/WE w zakresie integracji rejestrów centralnych, rejestrów handlowych i rejestrów spółek (określana jako dyrektywa BRIS).
2. Jabłoński A., Kawczyńska M., Pietrzak Ż., Wnuk-Pel T., *Oczekiwania wpływu implementacji zintegrowanego systemu informatycznego na jakość informacji – studium przypadku*, „Zeszyty Teoretyczne Rachunkowości" 2016, t. 89(145).
3. Oleśniewicz J., *JPK – wstęp do cyfryzacji rachunkowości i rewizji finansowej*, „Rachunkowość" 2016, 8.
4. Ramin K.P., Reiman C.A., *IFRS and XBRL*, WILEY, A.J. Willey &Sons, Publication, London 2013.
5. Rut J., Kulińska E., *Zintegrowany system informatyczny w przedsiębiorstwie produkcyjnym*, „Logistyka" 2013, 1.
6. Scapens R.W., Ezzamel M., Burns J., Baldvinsdottir G., *The Future Direction of UK Management Accounting Practice*, Elsevier/CIMA Publications, London 2003.

7. Siegel G., Sorensen J.E., *Counting More, Counting Less: The New Role of Management Accountants*, „Transformations in the Management Accounting Profession" 1999, vol. 3, Institute of Management Accountants.
8. Umble E.J., Haft R.R., Umble M., *Enteprise Resource Planning: Implementation Procedures and Critical Success Factors*, „European Journal of Operational Research" 2003, 146(2).
9. Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego, Dz.U. z 2016 r., poz. 1358.
10. Ustawa z dnia 29 września 1994 r. o rachunkowości, Dz.U. z 2016 r., poz. 615.
11. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne, Dz.U. z 2016 r., poz. 352.
12. Voss G., *Kształtowanie norm etycznych a odpowiedzialność zawodowa księgowych*, Wydawnictwo Uczelniane Uniwersytetu Technologiczno-Przyrodniczego w Bydgoszczy, Bydgoszcz 2016.
13. Voss G., Prewysz-Kwinto P., *Zintegrowane systemy ewidencyjne*, w: *Przyszłość rachunkowości i sprawozdawczości – założenia, zasady, definicje. Kierunki zmian prawa bilansowego w Polsce*, red. Z. Luty, A. Łakomiak, A. Mazur, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2013.
14. Zalewski W., *Analiza systemów informatycznych wspomagających zarządzanie produkcji w wybranych przedsiębiorstwach*, „Economy and Management" 2011, 4.

Źródła internetowe

1. http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915
2. https://mac.gov.pl/files/nask_rekomendacja.pdf

Accounting in the Process of Digitalisation. Risk Areas

Summary

The article includes basic assumptions connected with the implementation of digitalisation processes in accounting and the implementation of guidelines for the EU member states resulting from the Directive of the European Parliament and Council 2012/17/EU of 13 June 2012 amending the Council Directive 89/666/EEC and the Directive of the European Parliament and Council 2005/56/EC and 2009/101/EC with regard to the integration of central registers, trade registers and company registers. The description of new solutions related to the export of financial data and making e-applications is based on the amendments in the Polish legal regulations with the dates of their implementation taken into account. Furthermore, the article indicates benefits and threats resulting from the operation of business entities in the cyber space.

Keywords: Uniform Control File, digitalisation, tax information

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

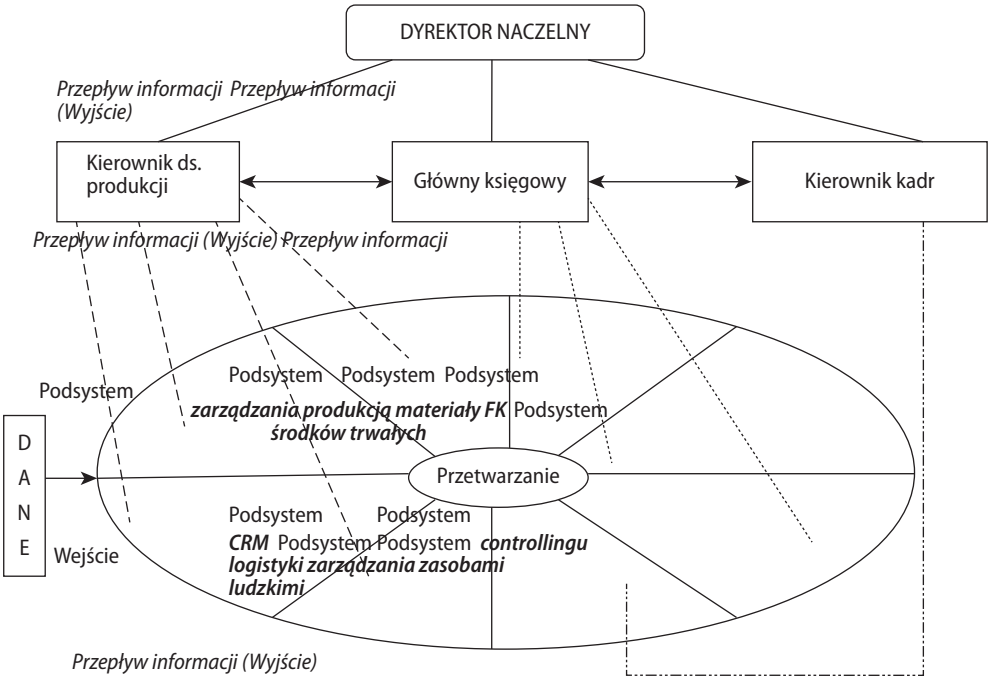
[10] K. Sawicki, *Podstawy rachunkowości*, PWE, Warszawa 2009, s. 15.

[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

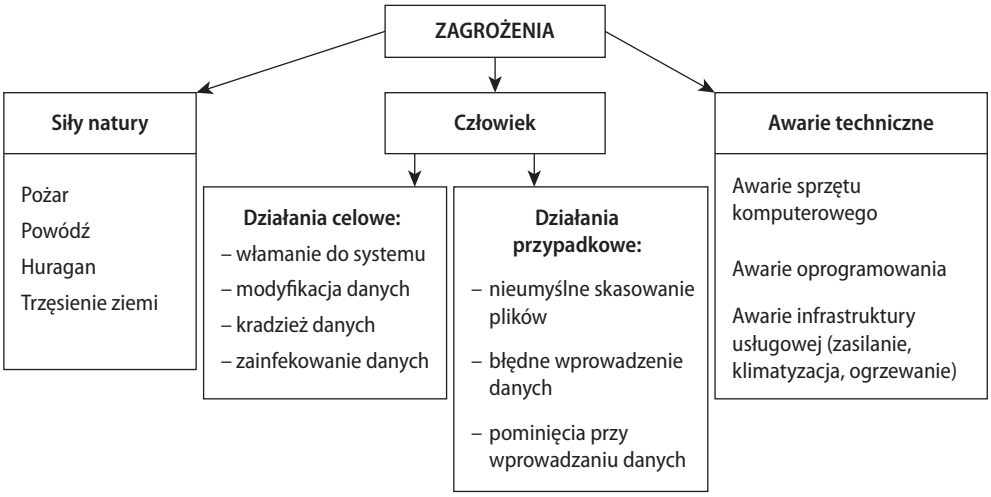
Jak zauważa J. Unold, elementem pierwotnym w stosunku do informacji są „dane", definiowane jako liczby i fakty wyrażone w określonej postaci znakowej, które mogą być przetworzone w informacje przy użyciu sprzętu komputerowego[15].

[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.

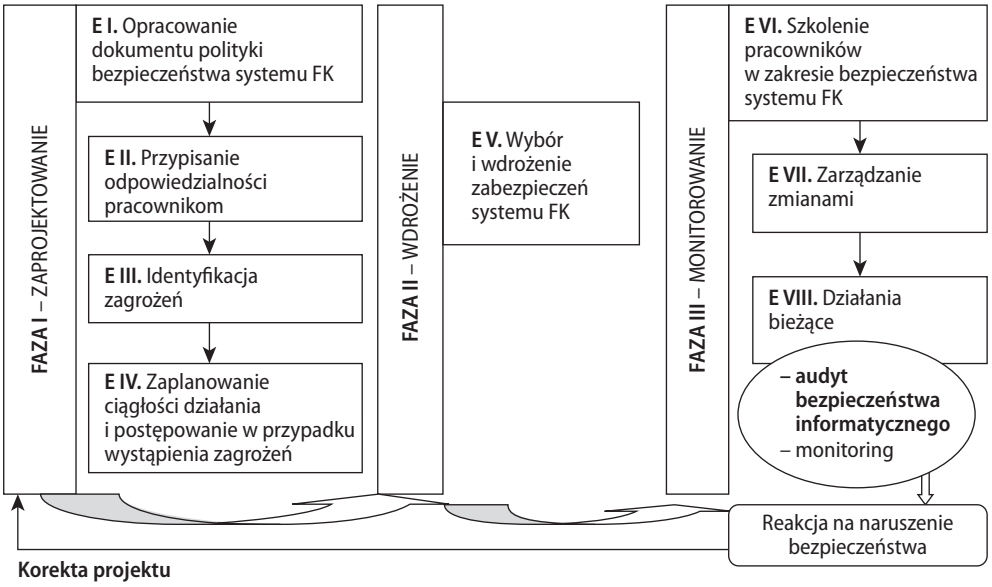
[22] J. Piotrowski, M. Szymaczek, *Projektowanie skutecznych systemów ochrony informacji*, „Informatyka" 1997, nr 7–8.

[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

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 69–87

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

Jolanta Wiśniewska
Uniwersytet Mikołaja Kopernika w Toruniu

Bezpieczeństwo informacji a ryzyko przestępczości komputerowej

Streszczenie

Rozwój nowych technologii oraz globalny rynek kształtują otaczającą nas rzeczywistość. Szczególnie dynamicznie ewoluują systemy komputerowe, w tym również systemy informatyczne rachunkowości. Rachunkowość jako jeden z najważniejszych elementów systemu informacyjnego jednostki gospodarczej jest szczególnie narażona na zagrożenia wynikające z rozwoju nowoczesnych technologii komputerowych i rynku globalnego. Celem artykułu jest przedstawienie uregulowań prawnych oraz zagrożeń, wynikających z rozwoju nowych technologii, dla działalności gospodarczej, a w szczególności dla systemu informacyjnego przedsiębiorstw, metod ich wykrywania i zapobiegania. W dobie ciągłych cyberataków liczą się przede wszystkim szybkie i sprawne działania w celu zapobiegania takim zagrożeniom, synchronizujące technologię, działania prawne i zarządzanie komunikacją. Cyberbezpieczeństwo przy tak dynamicznym rozwoju nowoczesnych technologii stało się strategiczną koniecznością.

Słowa kluczowe: rachunkowość, przestępczość komputerowa, rachunkowość śledcza, cyberbezpieczeństwo
Kody klasyfikacji JEL: M41, M48

1. Wprowadzenie

Według EY rozwój nowych technologii oraz globalnego rynku należą do sześciu globalnych megatrendów[1] kształtujących otaczającą nas rzeczywistość[2]. W szczególności szybkim rozwojem charakteryzują się zintegrowane systemy komputerowe typu ERP. Intensywny rozwój technologii informatycznych dotyczy również systemów informatycznych rachunkowości. Rachunkowość jest ważnym elementem systemu informacyjnego jednostki gospodarczej. Jest ona we współczesnym rozumieniu systemem informacyjnym, którego celem jest pomoc interesariuszom w procesie podejmowania decyzji gospodarczych, finansowych, jak również jest narzędziem, który ma za zadanie rozliczanie kierownictwa z zarządzania powierzonym mu mieniem[3]. Zatem jest ona w szczególności narażona na zagrożenia wynikające z rozwoju nowoczesnych technologii komputerowych i rynku globalnego. Według badań przeprowadzonych przez PwC liczba wykrytych incydentów naruszających bezpieczeństwo informacji w 2015 r. wzrosła na świecie w stosunku do roku poprzedniego o 38%, natomiast w Polsce aż o 46%[4].

Celem artykułu jest przedstawienie uregulowań prawnych oraz zagrożeń dla rachunkowości, wynikających z rozwoju nowych technologii, metod ich wykrywania i zapobiegania.

Do realizacji sformułowanego celu zastosowano następujące metody badawcze: studium literatury przedmiotu, analizę aktów prawnych regulujących zagadnienia dotyczące przestępstw komputerowych i cyberbezpieczeństwa, studium wyników badań dotyczących występowania cyberataków w Polsce i na świecie oraz metodę analizy przypadków dotyczących usług z zakresu cyberbezpieczeństwa organizacji.

---

[1] Megatrendy stanowią połączone globalne siły, mające wpływ na wszystkich ludzi poprzez zmianę społeczeństwa, kultury oraz gospodarki. Pozwalają na lepsze zrozumienie zarówno wyzwań, jak i szans stojących przed współczesnym biznesem, EY, *Megatrends 2015. Making Sense of a Word in Motion*, http://www.ey.com, dostęp 09.11.2016, s. 2; patrz także: PwC, *W obronie cyfrowych granic czyli 5 rad, aby realnie wzmocnić ochronę firmy przed CYBER ryzykiem*, Warszawa, https://www.pwc.pl, dostęp 10.11.2016, s. 4.

[2] EY, *Megatrends*…, op.cit., s. 2; patrz także: KPMG, *Future State 2030: Światowe wyzwania dla liderów i przywódców*, https://www.kpmg.com/PL/pl, dostęp 2.11.2016, s. 1–3; PwC, *W obronie*…, op.cit., s. 4.

[3] B. Kunz, A. Tymińska, *System informatyczny rachunkowości i jego rola w świetle ustawy o rachunkowości*, „Nauki o Finansach" 2014, nr 3(20), s. 44.

[4] PwC, *W obronie*…, op.cit., s. 4.

2. Rachunkowość jako system informacyjny przedsiębiorstw

Rachunkowość jako „międzynarodowy język biznesu”[5] była wielokrotnie definiowana. W tabeli 1 zostały przedstawione wybrane definicje pojęcia „rachunkowość”.

Tabela 1. Wybrane definicje pojęcia „rachunkowość”

Autor	Definicja pojęcia „rachunkowość”
W. Brzezin	System informacyjny organizacji gospodarczych o charakterze retro- i prospektywnym, który posiada własny algorytm rachunku ekonomicznego i metody ustalenia, planowania oraz analizy wyniku finansowego w pewnym okresie oraz kondycji finansowej w ściśle określonym momencie czasowym
E. Burzymowa	Uniwersalny, podmiotowy system informacyjno-kontrolny
S. Skrzywan	Ogół metod i zabiegów rachunkowych, systematycznych i dorywczych, stosowanych w przedsiębiorstwie celem stworzenia podstaw dla decyzji kierowniczych
A. Jarugowa	Pomiar oraz analiza relacji i interakcji związanych z przenoszeniem i tworzeniem, podziałem i ewentualnie utratą wartości, zarówno jako nośników użyteczności (wartości użytkowej), jak i mierników wartości. Współcześnie jest ona postrzegana jako prawnie regulowany, specyficzny system informacyjny, tworzący liczbową reprezentację sytuacji finansowej i wyników działalności podmiotu gospodarczego
S. Sojak	Pewien system identyfikacji, pomiaru, przetwarzania i przekazywania informacji finansowych o sytuacji majątkowej i osiąganych wynikach – służący celom sprawozdawczym i decyzyjnym różnych podmiotów (użytkowników)

Źródło: opracowanie własne na podstawie: W. Brzezin, *Rachunkowość sensu stricto i sensu largo*, „Zeszyty Teoretyczne Rachunkowości” 2000, t. 56, s. 18; E. Burzym, *Rachunkowość przedsiębiorstwa i instytucji*, PWE, Warszawa 1980, s. 13; S. Skrzywan, *Rachunkowość w przedsiębiorstwie przy gospodarce planowej. Cele i funkcje*, Prace Zakładu Rachunkowości SGH w Warszawie, nr 1, Gospodarczy Instytut Wydawniczy, Warszawa 1948, s. 11; A. Jarugowa, *Niektóre wyznaczniki rozwoju rachunkowości*, w: *Współczesne problemy rachunkowości*, red. A. Jarugowa, PWE, Warszawa 1991, s. 13; A. Jarugowa, *Wprowadzenie – istota zmian w ustawie o rachunkowości i ich skutki ekonomiczne*, w: *Komentarz do ustawy o rachunkowości. Rachunkowość – MSR – Podatki*, red. A. Jarugowa, T. Martyniuk, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 2002, s. 51; S. Sojak, *Pojęcie rachunkowości*, w: *Podstawy rachunkowości*, red. S. Sojak, J. Stankiewicz, TNOiK, Toruń 2008, s. 21.

Cechą wspólną wszystkich przedstawionych definicji pojęcia „rachunkowość” jest to, że stanowi ona system informacyjny, będący podstawą podejmowania decyzji. To jeden z najważniejszych elementów systemu informacyjnego przedsiębiorstwa,

[5] E.A. Hendriksen, M.F. van Breda, *Teoria rachunkowości*, Wydawnictwo Naukowe PWN, Warszawa 2002, s. 35; W. Brzezin, *Ogólna teoria rachunkowości*, Wyższa Szkoła Handlu i Prawa, Warszawa 1998, s. 22; E. Walińska, *Międzynarodowe Standardy Rachunkowości*, Oficyna Ekonomiczna, Kraków 2006, s. 15; J. Turyna, *Rachunkowość finansowa*, C.H. Beck, Warszawa 2005, s. 9–16.

ewoluuje wraz z jego rozwojem. Na globalnym konkurencyjnym rynku informacja w różnych przekrojach informacyjnych o charakterze zarówno retro- jak i prospektywnym[6] stała się nie tylko koniecznością, lecz także towarem, nie zawsze pozyskiwanym w sposób legalny.

Najbardziej efektywnym i najważniejszym narzędziem, który stanowi podstawę systemu informacyjnego rachunkowości, jest system informatyczny[7]. Wraz z rozwojem technologii również systemy informatyczne ewoluowały od prostych systemów finansowo-księgowych do systemów ERP.

W Polsce zasady prowadzenia ksiąg rachunkowych i sporządzania sprawozdań finansowych reguluje ustawa o rachunkowości[8]. Zgodnie z art. 10 ust. 1 ustawy, każda jednostka powinna posiadać dokumentację opisującą przyjęte przez nią zasady (politykę) rachunkowości, w tym zasady dotyczące prowadzenia ksiąg rachunkowych przy użyciu komputera. Ponadto dokumentacja ta powinna zawierać wykaz 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, z opisem systemu informatycznego zawierającego wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, wraz z wyjaśnieniem algorytmów i parametrów. Jednostki mają obowiązek zawarcia w polityce rachunkowości informacji dotyczącej wersji oprogramowania i daty rozpoczęcia jego eksploatacji. Ustawa reguluje także obowiązki w zakresie cech ksiąg rachunkowych prowadzonych z użyciem komputera, obowiązkowe elementy dotyczące zapisów księgowych i wydruków komputerowych oraz warunki uznania zapisów na trwałych nośnikach danych. Ważny element dokumentacji opisującej zasady prowadzenia ksiąg rachunkowych stanowi opis programowych zasad ochrony danych, w tym w szczególności metod zabezpieczenia dostępu do danych i systemu ich przetwarzania[9].

Rozwój technologii spowodował, że 57% informacji jest generowana wyłącznie w formie elektronicznej, a 43% w formie papierowej[10], co wymusza na organizacjach

---

[6] W. Brzezin, *Ogólna*…, op.cit., s. 18.

[7] Por. A. Jabłoński, M. Kawczyńska, Ż. Pietrzak, T. Wnuk-Pel, *Oczekiwany wpływ implementacji zintegrowanego systemu informatycznego na jakość informacji – studium przypadku*, „Zeszyty Teoretyczne Rachunkowości" 2016, t. 89(145), s. 57; B. Kunz, A. Tymińska, *System*…, op.cit., s. 44–45.

[8] Ustawa z dnia 29 września 1994 r. o rachunkowości, Dz.U. z 2016 r., poz. 1047 ze zm.

[9] Ibidem, art. 10, 13, 14.

[10] J. Góra, *Raport. Efektywne zarządzanie bezpieczeństwem informacji*, Ślązak, Zapiór i Wspólnicy, Media Recowery, https://www.us.edu.pl, dostęp 08.11.2016, s. 4.

stosowanie coraz bardziej zaawansowanych technologicznie zabezpieczeń. Uregulowania zawarte w ustawie o rachunkowości mają za zadanie systemowe zapewnienie bezpieczeństwa prowadzeniu ksiąg rachunkowych za pomocą komputera i ochronę danych, co przy aktualnej dynamice rozwoju technologicznego i globalizacji staje się priorytetem w walce z przestępczością komputerową.

3. Przestępczość komputerowa

Rozwój technologii komputerowych ma wpływ na współczesne życie i gospodarkę zarówno w skali mikro, jak i makro[11]. Ma on również wpływ na działalność przedsiębiorstw, kształtuje ich rozwój, a to z kolei na coraz większe zapotrzebowanie na wszelkiego rodzaju informacje. Z drugiej jednak strony, rozwój nowych technologii, do których można zaliczyć m.in. Internet, urządzenia mobilne, media społecznościowe, chmury obliczeniowe, duże zbiory danych (ang. *big data*), sprzyja powstawaniu coraz nowszych rodzajów przestępstw z ich udziałem bez ograniczeń terytorialnych[12]. Można zatem stwierdzić, że działalność gospodarcza prowadzona jest obecnie w erze cyberataków i kryzysu zaufania[13].

Opracowanie i wdrożenie właściwych aktów prawnych stanowi główny środek w przeciwdziałaniu rosnącym przypadkom cyberprzestępczości[14]. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW określa rodzaje zagrożeń dotyczących przestępczości komputerowej. Wykaz zagadnień, określanych mianem ataków na systemy informatyczne, przedstawiono w tabeli 2.

[11] Por. N. Kshetri, *Positive Externality, Increasing Returns, and the Rise in Cybercrimes*, „Communications of the ACM" 2009, vol. 52, no. 12, s. 141–144.

[12] Por. EY, *Megatrends…*, op.cit., s. 4; patrz także: N. Kshetri, *Positive…*, op.cit., s. 141–144.

[13] Por. PwC, *W obronie…*, s. 1.

[14] C. Barclay, *Using Frugal Innovations to Support Cybercrime Legislations in Small Developing States: Introducing the Cyber-Legislation Development and Implementation Process Model (CyberLeg-DPM)*, „Information Technology for Development" 2014, vol. 20, no. 2, 165–195; patrz także: K.L. Hui, S.H. Kim, Q.H. Wang, *Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks*, „MIS Quarterly" 2017, vol. 41, no. 2, s. 497–523.

Tabela 2. Cyberprzestępstwa – prawo unijne

Rodzaj przestępstwa komputerowego	Art.	Charakterystyka
Niezgodny z prawem dostęp do systemów informatycznych	3	Umyślne i bezprawne uzyskiwanie dostępu do całości lub jakiejkolwiek części systemu informatycznego
Niezgodna z prawem ingerencja w systemy	4	Umyślne i bezprawne poważne utrudnienie lub zakłócenie funkcjonowania systemu informatycznego poprzez wprowadzenie, przekazywanie, uszkadzanie, usuwanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych lub czynienie ich niedostępnymi
Niezgodna z prawem ingerencja w dane	5	Umyślne i bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi
Niezgodne z prawem przechwytywanie danych	6	Umyślne i bezprawne przechwytywanie środkami technicznymi niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego, w tym emisji elektromagnetycznych z systemu informatycznego zawierającego takie dane komputerowe

Źródło: opracowanie własne na podstawie: Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz.U. UE L 218 z dnia 14.08.2013 r.

Ogólne zagadnienia opisujące rodzaje przestępstw komputerowych określa prawo unijne, natomiast poszczególne kraje ustanawiają przepisy szczegółowe. Wybrane uregulowania prawne dotyczące przestępstw komputerowych w Polsce przedstawiono w tabeli 3.

Tabela 3. Cyberprzestępstwa – prawo polskie

Akt prawny	Przepis	Charakterystyka
Kodeks karny Rozdział XXXIII Przestępstwa przeciwko ochronie informacji	Art. 265	Nieuprawnione wykorzystanie informacji niejawnych o klauzuli „tajne" lub „ściśle tajne"
	Art. 266	Nieuprawnione ujawnianie lub wykorzystanie informacji w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową
	Art. 267	Uzyskanie dostępu do informacji przeznaczonych dla innych osób, polegające na otwieraniu zamkniętego pisma, podłączaniu się do sieci telekomunikacyjnej lub przełamywaniu albo omijaniu elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń
	Art. 268	Niszczenie, uszkadzanie, usuwanie lub zmiana zapisów istotnej informacji albo w inny sposób udaremnianie lub znaczne utrudnianie osobie uprawnionej zapoznania się z nią

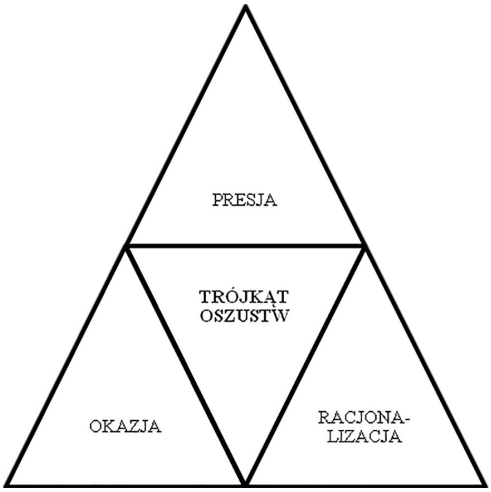
Akt prawny	Przepis	Charakterystyka
Kodeks karny Rozdział XXXIII Przestępstwa przeciwko ochronie informacji	Art. 268a	Niszczenie, uszkadzanie, usuwanie, zmiana lub utrudnianie dostępu do danych informatycznych albo w istotnym stopniu zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych
	Art. 269	Niszczenie, uszkadzanie, usuwanie lub zmiana danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Niszczenie poprzez wymianę informatycznych nośników danych lub przez uszkodzenie urządzeń służących do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych
	Art. 269a	Przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej
	Art. 269b	Wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzenia lub programu komputerowego przystosowanego do popełnienia przestępstwa, a także hasła komputerowego, kodu dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej
Ustawa o zwalczaniu nieuczciwej konkurencji	Art. 23	Ujawnianie innej osobie lub wykorzystanie we własnej działalności gospodarczej informacji stanowiących tajemnicę przedsiębiorstwa uzyskanych w związku z pełnioną funkcją lub uzyskanych bezprawnie
Ustawa o ochronie danych osobowych	Art. 49	Przetwarzanie danych osobowych w zbiorze bez prawa przetwarzania tych danych
	Art. 52	Przy administrowaniu danymi naruszanie choćby nieumyślnie obowiązku zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem
	Art. 53	Niezgłaszanie do rejestracji zbioru danych przez osoby obowiązane

Źródło: opracowanie własne na podstawie: Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r. nr 88 poz. 533 ze zm.; Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. z 2003 r. nr 153, poz. 1503 ze zm.; Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2015 r., poz. 2135 ze zm.

Według D.R. Cresseya oszustwa dotyczące działalności gospodarczej, a szczególnie systemu informacyjnego organizacji, opierają się na tzw. trójkącie oszustw[15], który został przedstawiony na rysunku 1.

[15] J.T. Wells, *Nadużycia w firmach. Vademecum. Zapobieganie i wykrywanie*, LexisNexis, Warszawa 2006, s. 6–15.

Rysunek 1. Trójkąt oszustw



Źródło: opracowanie własne na podstawie: J.T. Wells, *Nadużycia w firmach. Vademecum. Zapobieganie i wykrywanie*, LexisNexis, Warszawa 2006, s. 7.

Trójkąt oszustw ma również zastosowanie do cyberataków. Ryzyko jest tym większe, im więcej występuje słabych stron w organizacji systemu informacyjnego przedsiębiorstwa, co stwarza okazje dla przestępców. W badaniach przeprowadzonych przez EY[16] respondenci dokonali oceny słabych stron organizacji systemu informacyjnego, mających wpływ na zwiększenie ryzyka cyberataków. Ocena 1 oznaczała największe ryzyko, a ocena 5 najmniejsze (tabela 4).

Z badań przedstawionych w tabeli 4 wynika, że największym zagrożeniem dla powstawania cyberataków w pierwszej kolejności jest czynnik ludzki, czyli niestaranni i nieświadomi pracownicy, których działania lub brak działań w największym stopniu wpływają na wzrost ryzyka powstawania przestępstw komputerowych. W następnej kolejności największa liczba respondentów wskazała na brak aktualnych kontroli bezpieczeństwa informacji lub jej architektury. Z analizy czynników

[16] Badanie EY było skierowane do dyrektorów ochrony informacji, dyrektorów finansowych, prezesów i innych menedżerów zajmujących się ochroną informacji. Zostało przeprowadzone w okresie od czerwca do września 2015 r. W badaniu wzięło udział 1755 respondentów z 67 krajów, reprezentujących 25 głównych gałęzi przemysłu, którzy otrzymali kwestionariusz ankietowy. Większość odpowiedzi zebrano podczas wywiadów „face to face". Gdy nie było to możliwe, kwestionariusz został wypełniony przez Internet, EY, *Creating trust in the digital world. EY's Global Information Security Survey 2015*, http://www.ey.com, dostęp 9.11.2016, s. 30–31.

o największym ryzyku należy stwierdzić, iż są to czynniki wynikające z wewnętrznej struktury organizacji systemu informacyjnego, a dopiero na końcu z racji korzystania z mediów publicznych. Potwierdza to ocena respondentów dotycząca najmniejszego ryzyka, gdzie największa liczba respondentów wskazała na użytkowanie publicznych mediów społecznościowych i korzystanie z publicznej (niezabezpieczonej) chmury obliczeniowej (po 23%). Przy analizie tabeli 4 narzuca się wniosek, że pomimo wzrastającego zagrożenia przestępczością komputerową, największa liczba ocen dotycząca czynników stanowiących słabe punkty organizacji została oceniona na poziomie średniego ryzyka (ocena 3).

Tabela 4. Słabe strony organizacji systemu informacyjnego przedsiębiorstw (w %)

Ocena / Słabe punkty	1	2	3	4	5
Użytkowanie publicznych mediów społecznościowych*	6	14	31	25	23
Korzystanie z publicznej (niezabezpieczonej) chmury obliczeniowej	10	18	28	21	23
Korzystanie z mobilnych aplikacji komputerowych	9	23	31	22	15
Nieaktualne kontrole bezpieczeństwa informacji lub jej architektury	15	19	31	19	16
Nieautoryzowany dostęp	10	22	36	20	12
Niestaranni lub nieświadomi pracownicy*	18	26	32	14	9

* Dane z badania nie sumują się do 100%.

Źródło: opracowanie własne na podstawie: EY, *Creating Trust in the Digital World. EY's Global Information Security Survey 2015*, http://www.ey.com, dostęp 9.11.2016, s. 6.

Ważnym zagadnieniem dotyczącym wykrywalności cyberataków jest identyfikacja ich sprawców. Badania przeprowadzone przez PwC[17] wskazały główne źródła ataków, co zostało zaprezentowane w tabeli 5.

W tabeli 5 przedstawiono strukturę sprawców przestępstw komputerowych w Polsce na tle świata – zarówno w Polsce, jak i na świecie głównymi sprawcami cyberataków byli pracownicy. Również inne wyniki badań oraz literatura przedmiotu potwierdzają wiodącą rolę pracowników wśród sprawców cyberataków[18]. Natomiast

[17] W badaniu przeprowadzonym przez PwC wzięło udział 126 polskich ekspertów zajmujących się IT i bezpieczeństwem informacji. Zostało one przeprowadzone jesienią 2015 r. metodą ankiety *online*, PwC, *W obronie*…, op.cit., s. 23.

[18] Por. J. Mayer, *Cybercrime Litigation*, „University of Pennsylvania Law Review" 2016, vol. 164, s. 1502; KPMG, *Profil korporacyjnego oszusta*, https://assets.kpmg.com, dostęp 15.11.2016, s. 21; J. Góra, *Raport*…, op.cit., s. 11–12; EY, *Creating*…, op.cit., s. 12.

jeżeli chodzi o pozostałe grupy cyberprzestępców, to ich struktura kształtowała się odmiennie. W Polsce w drugiej kolejności sprawcą cyberataków byli nieznani hakerzy, następnie przestępcy z grup zorganizowanych i ostatnią główną grupą byli obecni dostawcy i wykonawcy. Odmiennie kształtowała się struktura sprawców przestępstw komputerowych na świecie: w drugiej kolejności odnotowano incydenty z udziałem byłych pracowników, a następnie obecnych dostawców i wykonawców.

Tabela 5. Główni sprawcy cyberataków w 2015 r. (w %)

Wyszczególnienie	Polska	Świat
Pracownicy	70	34
Byli pracownicy	–	29
Nieznani hakerzy	67	–
Przestępcy z grupy zorganizowanej	41	–
Obecni dostawcy i wykonawcy	35	19

Źródło: opracowanie własne na podstawie: PwC, *W obronie cyfrowych granic, czyli 5 rad, aby realnie wzmocnić ochronę firmy przed CYBER ryzykiem*, https://www.pwc.pl, dostęp 10.11.2016, s. 10.

W wyniku cyberataków jednostka ponosi wiele konsekwencji, które mają na nią wpływ zarówno w krótkim, jak i dłuższym okresie. Do konsekwencji tych należą m.in. nadszarpnięcie reputacji i marki jednostki, poniesienie przez jednostkę odpowiedzialności cywilnej, wystąpienie zagrożeń dla działalności przedsiębiorstwa, powstanie szkód finansowych, naruszenie interesów klientów/kontrahentów czy też ukaranie osób odpowiedzialnych za bezpieczeństwo informacji w firmach[19]. Konsekwencje cyberprzestępczości w polskich firmach przedstawiono w tabeli 6.

Tabela 6. Konsekwencje cyberataków w polskich firmach w 2015 r.

Wyszczególnienie	Udział w %
Utrata klientów	33
Straty finansowe	33
Ujawnianie lub modyfikacja danych	31
Utrata reputacji	16

Źródło: jak pod tab. 5, s. 8.

[19] Por. J. Góra, *Raport…*, op.cit., s. 9.

Z wyników badań przedstawionych w tabeli 6 wynika, że w polskich firmach skutkami cyberataków są prawie w takim samym stopniu utrata klientów, straty finansowe oraz ujawnianie lub modyfikacja danych.

4. Działania dotyczące cyberbezpieczeństwa w firmach

W dobie ciągłych cyberataków liczy się przede wszystkim szybka i sprawna reakcja na incydenty. Taka, która synchronizuje technologię, działania prawne i zarządzanie komunikacją[20]. Ponad 77% organizacji zdaje sobie sprawę z wartości posiadanych przez nich informacji, a to z kolei ma wpływ na coraz większą świadomość potrzeby działań prewencyjnych[21]. Według badań przeprowadzonych przez KPMG w 2015 r. 29% prezesów firm wymienia cyberbezpieczeństwo jako problem, który ma obecnie największy wpływ na funkcjonowanie firm[22].

Bardzo ważne dla bezpieczeństwa informacji jest zrozumienie wyzwań z tym związanych. Według EY w celu skutecznego rozpoznania i odpowiedniej reakcji na niebezpieczeństwa związane z cyberprzestępczością, organizacje muszą posiadać odpowiednią wiedzę i zrozumieć ich istotę. Każda jednostka powinna posiadać informacje na temat aktualnych rodzajów cyberataków, w jaki sposób te ataki są przeprowadzane, jak jest do tego przygotowana i jak można temu przeciwdziałać[23].

W badaniach przeprowadzonych przez EY respondenci dokonali oceny ryzyka występowania zagrożeń dotyczących systemu informacyjnego organizacji; ocena 1 oznaczała największe ryzyko, a ocena 5 najmniejsze (tabela 7).

Największe zagrożenie, zdaniem respondentów (19%) stanowi ryzyko wyłudzania informacji, na drugim miejscu znalazły się zagrożenia dotyczące złośliwego oprogramowania i ataków typu „godzina-zero" (po 16%), a na trzecim wskazane zostały ryzyko cyberataków dotyczących kradzieży informacji finansowych i zakłócających

[20] PwC, *W obronie*…, op.cit., s. 1.

[21] J. Góra, *Raport*…, op.cit., s. 4.

[22] Dane oparte zostały na badaniu ankietowym przeprowadzonym wśród 1276 prezesów firm z Australii, Chin, Francji, Niemiec, Indii, Włoch, Japonii, Hiszpanii, Wielkiej Brytanii i USA. Respondenci reprezentowali dziewięć kluczowych branż: motoryzację, bankowość, ubezpieczenia, zarządzanie inwestycjami, opiekę zdrowotną, technologię, handel detaliczny / rynki konsumenckie, energetykę oraz usługi komunalne; KPMG, *Cyberbezpieczeństwo – wyzwanie współczesnego prezesa*, https://assets.kpmg.com, dostęp 8.11.2016, s. 4.

[23] EY, *Creating*…, op.cit., s. 2; patrz także Deloitte, *Beneath the Surface of a Cyberattack. A Deeper Look at Business Impacts*, https://www².deloitte.com, dostęp 15.11.2016, s. 2.

pracę organizacji lub niszczących organizację (po 15%). Zdaniem respondentów najmniejsze zagrożenie dla systemu informacyjnego organizacji stanowią klęski żywiołowe (35%). Natomiast najmniejsze ryzyko cyberataków dotyczy kradzieży informacji finansowych. Takie wskazanie respondentów może mieć swoje uzasadnienie wymogami prawnymi, które ich zdaniem, wymuszają na jednostkach opracowanie i wdrożenie procedur bezpieczeństwa informacji.

Tabela 7. Zagrożenia systemu informacyjnego organizacji (w %)

Zagrożenia \ Ocena	1	2	3	4	5
Klęski żywiołowe (huragany, powodzie itp.)	9	11	23	22	35
Szpiegostwo (np. przez konkurencję)	9	14	24	22	31
Cyberataki dotyczące kradzieży własności intelektualnej lub danych	13	17	26	22	21
Ataki wewnętrzne (np. przez niezadowolonych pracowników)	9	18	32	23	19
Cyberataki dotyczące kradzieży informacji finansowych	15	18	25	19	23
Cyberataki zakłócające pracę organizacji lub niszczące organizację	15	18	29	19	19
Oszustwa	12	22	28	19	19
Spamy	9	19	36	22	13
Ataki typu „godzina-zero"	16	19	32	16	17
Wyłudzanie informacji	19	25	29	16	12
Złośliwe (szkodliwe) oprogramowanie (np. wirusy, robaki i konie trojańskie)	16	27	30	18	9

Źródło: jak pod tab. 4, s. 6.

Po dokonaniu analizy ryzyka poszczególnych zagrożeń dotyczących cyberataków, organizacja powinna przystąpić do działań mających za zadanie przeciwdziałanie/obronę przed tego typu incydentami. Wdrożenie systemu zarządzania ryzykiem jest istotnym elementem bezpieczństwa informacji. EY zidentyfikowało trzy fundamentalne bloki budowania cyberbezpieczeństwa (tabela 8).

Pomimo świadomości i wdrażania w przedsiębiorstwach rozwiązań dotyczących cyberbezpieczeństwa informacji, skuteczność działania stosowanych rozwiązań bardzo często jest niewystarczająca. Badania przeprowadzone przez EY wskazały na ograniczenia mające wpływ na skuteczność ochrony informacji (tabela 9).

Tabela 8. Fundamenty budowania cyberbezpieczeństwa w firmie

Podstawowe fundamenty cyberbezpieczeństwa	Charakterystyka
Przewidywanie (ang. *anticipate*)	Organizacje powinny budować solidne fundamenty cyberbezpieczeństwa, które powinny obejmować kompleksowy zestaw środków bezpieczeństwa informacji, będących podstawą obrony przed cyberatakami. Na tym etapie organizacje ustalają podstawy cyberbezpieczeństwa w firmie
Dostosowanie się (ang. *adapt*)	Organizacje w celu przetrwania na konkurencyjnym rynku powinny dostosowywać się do zmieniających się warunków. W związku ze zmianami w działalności gospodarczej również zagrożenia ulegają ewolucji, dlatego podstawą środków bezpieczeństwa informacji powinno być nadążanie za zmianami, ponieważ inaczej z upływem czasu staną się coraz mniej skuteczne. Na tym etapie jednostki powinny dostosować organizację cyberbezpieczeństwa do zmieniających się wymagań
Aktywacja (ang. *activate*)	Organizacje muszą opracować taktykę wykrywania i zmniejszenia ryzyka potencjalnych cyberataków. Muszą określić swoje potrzeby dotyczące ochrony swoich najcenniejszych aktywów i opracować scenariusze odpowiedzi na prawdopodobne zagrożenia cybernetyczne, co wymaga od nich zdolności wywiadowczych, opracowania metodologii oceny ryzyka, odpowiednich mechanizmów reagowania na incydenty i odpowiedniej organizacji. Na tym etapie jednostki określają swoją zdolność do obrony przed cyberzagrożeniami i niespodziewanymi atakami, jak również przewidują tego typu incydenty

Źródło: opracowanie własne na podstawie: EY, *Cybersecurity and the Internet of Things*, http://www.ey.com, dostęp 14.11.2016, s. 20.

Tabela 9. Przeszkody dotyczące skuteczności ochrony informacji

Wyszczególnienie	Udział w %
Ograniczenia budżetowe	62
Brak wykwalifikowanych zasobów	57
Brak świadomości wykonawczej lub wsparcia	32
Brak odpowiedniej jakości narzędzi do zarządzania bezpieczeństwem informacyjnym	28
Brak prawidłowego zarządzania	28
Fragmentacja dotycząca regulacji zgodności	23
Inne	7

Źródło: jak pod tab. 4, s. 26.

Z przedstawionych w tabeli 9 rezultatów badań wynika, że największą barierą jest przeznaczenie zbyt małego budżetu na bezpieczeństwo informacji. Potwierdzają to badania przeprowadzone przez PwC, z których wynika, że firmy polskie przeznaczają zaledwie 10% budżetu przeznaczonego na IT na cyberbezpieczeństwo

w stosunku do 19% na świecie[24]. Następne bariery dotyczą czynnika ludzkiego, a przede wszystkim braku osób z odpowiednimi kwalifikacjami (57%), a w następnej kolejności jest brak świadomości dotyczących zagrożeń komputerowych (32%). Istotnymi barierami są również brak skutecznych narzędzi i nieprawidłowa organizacja systemu bezpieczeństwa cybernetycznego.

W związku z rozwojem technologii, a w ślad za tym również technik przestępczości, same organizacje bardzo często nie są w stanie sobie z tym poradzić. Niewiele z nich posiada pracowników z odpowiednimi umiejętnościami i zasoby, które umożliwiałyby skuteczne zabezpieczenie firmy przed zagrożeniami wynikającymi z przestępczości komputerowej. Rozwiązaniem tego problemu może być współpraca z innymi organizacjami tej samej branży[25] bądź skorzystanie z zewnętrznego wsparcia, jakie można uzyskać od firm, które posiadają wysoko wykwalifikowanych pracowników[26], duże doświadczenie pozyskane w różnych branżach oraz odpowiednie narzędzia organizacyjne i techniczne.

Przykłady usług dotyczących rachunkowości śledczej i cyberbezpieczeństwa, których zadaniem jest obrona przed cyberatakami, ich wykrywanie, przygotowywanie odpowiednich procedur i kształtowanie kultury organizacyjnej bardziej otwartej w cyberprzestrzeni, a jednocześnie odpornej na przestępczość komputerową, przedstawiono w tabeli 10.

Przedstawione w tabeli 10 usługi można zaliczyć do rachunkowości śledczej. Wyspecjalizowane firmy oferują szeroki zakres usług, w celu przygotowania organizacji na cyberataki, jak również budowania sformalizowanej struktury bezpieczeństwa cybernetycznego. Polska należy do krajów o niskim poziomie cyberbezpieczeństwa w porównaniu z organizacjami światowymi. Obecnie w Polsce sformalizowany system zabezpieczeń ma 46% firm w stosunku do firm światowych, gdzie ma je 91% organizacji[27].

Dodatkowym zabezpieczeniem przed skutkami cyberataków mogą być ubezpieczenia dotyczące ich skutków, które mogłyby zminimalizować szkody powstałe w wyniku tego typu incydentów. W Polsce ten typ zabezpieczeń nie jest jeszcze zbyt powszechny, w badaniach przeprowadzonych przez PwC zaledwie 8% firm

[24] PWC, *W obronie…*, op.cit., s. 7.

[25] Z badań przeprowadzonych przez PWC wynika, że 45% organizacji nawiązuje taką współpracę, PwC, *W obronie…*, op.cit., s. 18.

[26] Por. K.T. Smith, L.M. Smith, J.L. Smith, *Case Studies of Cybercrime and Their Impact on Marketing Activity and Shareholder Value*, „Academy of Marketing Studies Journal" 2011, vol. 15, no. 2, s. 76.

[27] PwC, *W obronie…*, op.cit., s. 9.

biorących udział w badaniu zadeklarowało zawarcie polisy ubezpieczeniowej od następstw cyberataków, natomiast w przypadku badań światowych takie ubezpieczenie zakupiło 59% firm[28].

Tabela 10. Przykłady usług dotyczących cyberbezpieczeństwa

Rodzaj oferowanej usługi	Przykładowy zakres działań
Informatyka śledcza	• Stworzenie planu i zarządzanie procesem zabezpieczenia dysków twardych, taśm i dowodów cyfrowych, zgodnie z zasadami zabezpieczania materiału dowodowego • Odszukanie i gromadzenie danych elektronicznych, niezależnie od tego, gdzie się znajdują • Odtwarzanie historycznego stanu danych – przywracanie bazy danych systemu finansowego do stanu z przeszłości w poszukiwaniu dowodów popełnienia nadużyć • Identyfikacja, odzyskiwanie, zabezpieczanie oraz analiza dowodów elektronicznych zapisanych na różnego rodzaju nośnikach oraz w dowolnej konfiguracji • Przeanalizowanie materiału dowodowego w celu zlokalizowania, identyfikacji i wydobycia informacji mającej wartość dla dochodzenia lub sporu • Wykrywanie przypadków korupcji oraz malwersacji finansowych • Ujawnienie manipulacji sprawozdawczością finansową • Identyfikacja kradzieży majątku • Identyfikacja oszustw pracowniczych • Identyfikacja kradzieży danych • Ujawnienie konfliktów interesu (pracownicy – dostawcy) • Identyfikacja pracowników zamieszanych w oszustwa • Rozszerzenie wiedzy odnośnie do ryzyka, na które narażona jest spółka • Zbieranie publicznie dostępnych informacji o podmiotach i osobach, sposobach oraz strategiach działania osób i podmiotów stanowiących przedmiot zainteresowania klientów
Śledcza analiza danych	• Przeprowadzanie zaawansowanych analiz danych w zakresie dużych wolumenów transakcji i danych zawartych w systemach finansowo-księgowych, systemach CRM oraz systemach naliczania i wypłaty prowizji, w celu identyfikacji zdarzeń niewidocznych przy wykorzystaniu innego typu analiz • Badanie jakości i spójności danych, w tym analiza praktyk zarządzania danymi • Odnajdywanie zależności między pozornie niepowiązanymi źródłami danych • Identyfikacja sygnałów ostrzegawczych, które mogą świadczyć o wystąpieniu nadużyć • Analiza i mapowanie ryzyka w poszczególnych obszarach na podstawie indywidualnie dobranych kryteriów • Przewidywanie zagrożeń przyszłych nadużyć na podstawie analizy danych historycznych

[28] Ibidem, s. 18.

Rodzaj oferowanej usługi	Przykładowy zakres działań
Odzyskiwanie usuniętych danych i przeszukiwanie zbiorów komputerowych	• Zabezpieczanie elektroniczne danych komputerów, tabletów oraz telefonów komórkowych • Odzyskiwanie usuniętych informacji oraz ich szczegółowa analiza
Wdrażanie nowych narzędzi	• Wsparcie we wdrażaniu technologii służącej minimalizowaniu ryzyka nadużyć oraz prania pieniędzy
Cyberbezpieczeństwo	• Wykrywanie i odpowiedź na cyberzagrożenia • Ocena istniejącego środowiska bezpieczeństwa • Budowanie programu ochrony cybernetycznej – ochrona danych i prywatności • Zarządzanie cyberbezpieczeństwem

Źródło: opracowanie własne na podstawie: Deloitte, *Usługi. Zarządzanie ryzykiem nadużyć i zgodnością*, http://www2.deloitte.com/pl, dostęp 9.03.2016; E&Y, *Zarządzanie ryzykiem nadużyć*, http://www.ey.com/PL/pl, dostęp 8.03.2016; KPMG, *Zarządzanie ryzykiem nadużyć*, http://www.kpmg.com/PL/pl, dostęp 9.03.2016; PwC, *Usługi Forensic*, http://www.pwc.pl, dostęp 9.03.2016.

5. Podsumowanie

Cyberprzestępczość stanowi zagrożenie dla każdej, nawet najmniejszej organizacji. Poszczególne jednostki posiadają informacje, które mogą być atrakcyjne dla potencjalnego przestępcy. Przestępczość komputerowa zatem dotyczy każdej jednostki, natomiast dotychczasowe badania nad cyberprzestępczością dotyczyły w przeważającej części tylko największych organizacji, zatem nie odpowiadają one rzeczywistej skali tego zjawiska. Szczególnie odnosi się do specyfiki polskiego rynku, gdzie 99,8% jednostek stanowią małe i średnie przedsiębiorstwa[29]. Dla przedstawienia wielkości strat, jak również sposobów przeciwdziałania tego typu zjawiskom dalsze badania dotyczące Polski powinny objąć również przedsiębiorstwa sektora małych i średnich przedsiębiorstw.

W dobie cyfrowego świata działalność gospodarcza, dzięki postępowi technicznemu i stosowaniu różnych narzędzi, takich jak: urządzenia mobilne, Internet, media społecznościowe czy też chmury obliczeniowe, staje się bardziej otwarta, nie jest chroniona żadnymi granicami. Zdobycze techniki są z jednej strony lokomotywą rozwoju przedsiębiorstw, z drugiej stają się narzędziem w rękach przestępców. Zagrożenia wynikające z zastosowania nowoczesnych technologii wymuszają na ustawodawcach uchwalanie uregulowań prawnych, uwzględniających powstawanie

[29] PARP, *Raport o stanie sektora MSP w Polsce*, Polska Agencja Rozwoju Przedsiębiorczości, https://www.parp.gov.pl, dostęp 18.07.2017, s. 7.

coraz to nowszych rodzajów nadużyć z użyciem nowoczesnych technologii. Ponadto wymuszają na przedsiębiorstwach wprowadzenie rozwiązań systemowych dotyczących bezpieczeństwa informacji w celu ograniczenia występowania tego typu incydentów i zminimalizowania strat powstałych w ich wyniku. W Polsce brak jest badań dotyczących wpływu uregulowań prawnych na cyberataki oraz na wprowadzanie przez przedsiębiorstwa nowych rozwiązań systemowych.

W świecie cyfryzacji i globalizacji cyberbezpieczeństwo przestało być trendem, natomiast stało się strategiczną koniecznością każdej organizacji[30].

Bibliografia

Dokumenty prawne

1. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz.U. UE L 218 z dnia 14.08.2013 r.
2. Ustawa z dnia 29 września 1994 r. o rachunkowości, Dz.U. z 2016 r., poz. 1047 ze zm.
3. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. z 2003 r., nr 153, poz. 1503 ze zm.
4. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r. nr 88, poz. 553 ze zm.
5. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2015 r., poz. 2135 ze zm.

Wydawnictwa zwarte

1. Barclay C., *Using Frugal Innovations to Support Cybercrime Legislations in Small Developing States: Introducing the Cyber-Legislation Development and Implementation Process Model (CyberLeg-DPM)*, „Information Technology for Development" 2014, vol. 20, no. 2.
2. Brzezin W., *Ogólna teoria rachunkowości*, Wyższa Szkoła Handlu i Prawa, Warszawa 1998.
3. Brzezin W., *Rachunkowość sensu stricto i sensu largo*, „Zeszyty Teoretyczne Rachunkowości" 2000, t. 56.
4. Burzym E., *Rachunkowość przedsiębiorstwa i instytucji*, PWE, Warszawa 1980.
5. Hendriksen E.A., van Breda M.F., *Teoria rachunkowości*, Wydawnictwo Naukowe PWN, Warszawa 2002.

[30] PwC, *W obronie*…, op.cit., s. 1.

6. Hui K.L., Kim S.H., Wang Q.H., *Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks*, „MIS Quarterly" 2017, vol. 41, no. 2.
7. Jabłoński A., Kawczyńska M., Pietrzak Ż., Wnuk-Pel T., *Oczekiwany wpływ implementacji zintegrowanego systemu informatycznego na jakość informacji – studium przypadku*, „Zeszyty Teoretyczne Rachunkowości" 2016, t. 89(145).
8. Jarugowa A., *Niektóre wyznaczniki rozwoju rachunkowości*, w: *Współczesne problemy rachunkowości*, red. A. Jarugowa, PWE, Warszawa 1991.
9. Jarugowa A., *Wprowadzenie – istota zmian w ustawie o rachunkowości i ich skutki ekonomiczne*, w: *Komentarz do ustawy o rachunkowości. Rachunkowość – MSR – Podatki*, red. A. Jarugowa, T. Martyniuk, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 2002.
10. Kshetri N., *Positive Externality, Increasing Returns, and the Rise in Cybercrimes*, „Communications of the ACM" 2009, vol. 52, no. 12.
11. Kunz B., Tymińska A., *System informatyczny rachunkowości i jego rola w świetle ustawy o rachunkowości*, „Nauki o Finansach" 2014, nr 3(20).
12. Mayer J., *Cybercrime Litigation*, „University of Pennsylvania Law Review" 2016, vol. 164.
13. Skrzywan S., *Rachunkowość w przedsiębiorstwie przy gospodarce planowej. Cele i funkcje*, Prace Zakładu Rachunkowości SGH w Warszawie, nr 1, Gospodarczy Instytut Wydawniczy, Warszawa 1948.
14. Smith K.T., Smith L.M., Smith J.L., *Case Studies of Cybercrime and Their Impact on Marketing Activity and Shareholder Value*, „Academy of Marketing Studies Journal", 2011, vol. 15, no. 2.
15. Sojak S., *Pojęcie rachunkowości*, w: *Podstawy rachunkowości*, red. S. Sojak, J. Stankiewicz, TNOiK, Toruń 2008.
16. Turyna J., *Rachunkowość finansowa*, C.H. Beck, Warszawa 2005.
17. Walińska E., *Międzynarodowe Standardy Rachunkowości*, Oficyna Ekonomiczna, Kraków 2006.
18. Wells J.T., *Nadużycia w firmach. Vademecum. Zapobieganie i wykrywanie*, LexisNexis, Warszawa 2006.

Materiały internetowe

1. Deloitte, *Beneath the Surface of a Cyberattack. A Deeper Look at Business Impacts*, https://www2.deloitte.com
2. Deloitte, *Usługi. Zarządzanie ryzykiem nadużyć i zgodnością*, http://www2.deloitte.com/pl
3. EY, *Creating Trust in the Digital World. EY's Global Information Security Survey 2015*, http://www.ey.com

4. EY, *Cybersecurity and the Internet of Things*, http://www.ey.com
5. EY, *Megatrends 2015. Making Sense of a Word in Motion*, http://www.ey.com
6. EY, *Zarządzanie ryzykiem nadużyć*, http://www.ey.com/PL/pl
7. Góra J., *Raport. Efektywne zarządzanie bezpieczeństwem informacji*, Ślązak, Zapiór i Wspólnicy, Media Recowery, https://www.us.edu.pl
8. KPMG, *Cyberbezpieczeństwo – wyzwanie współczesnego prezesa*, https://assets.kpmg.com
9. KPMG, *Future State 2030: Światowe wyzwania dla liderów i przywódców*, https://www.kpmg.com/PL/pl/
10. KPMG, *Profil korporacyjnego oszusta*, https://assets.kpmg.com
11. KPMG, *Zarządzanie ryzykiem nadużyć*, http://www.kpmg.com/PL/pl
12. PARP, *Raport o stanie sektora MSP w Polsce*, Polska Agencja Rozwoju Przedsiębiorczości, https://www.parp.gov.pl
13. PwC, *Usługi Forensic*, http://www.pwc.pl
14. PwC, *W obronie cyfrowych granic, czyli 5 rad, aby realnie wzmocnić ochronę firmy przed CYBER ryzykiem*, https://www.pwc.pl

Information Security and Computer Crime Risk

Summary

The development of new technologies and the global market affect the surrounding reality. It is the computer systems, including the IT accounting systems that evolve especially dynamically. Accounting, as one of the most important elements of the information system of a business entity is particularly exposed to the threats resulting from the development of modern computer technologies and the global market. The article aims at the presentation of legal regulations as well as threats to the business pursuit resulting from the development of new technologies, in particular to the corporate information systems as well as the methods of their detection and prevention. At the age of continuous cyberattacks, it is essential to pursue immediate and efficient actions in order to prevent such threats to synchronise technology, legal procedures and communication management. Cybersecurity has become a sheer necessity in view of such a dynamic development of modern technologies.

Keywords: accounting, computer crime, forensic accounting, cybersecurity

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 89–105

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

Beata Dratwińska-Kania
Uniwersytet Ekonomiczny w Katowicach

Koszty cyberprzestępczości – perspektywa rachunkowości

Streszczenie

Z uwagi na postępującą informatyzację w różnych aspektach działalności przedsiębiorstwa, określenie, czym dokładnie są cyberprzestrzeń i koszty cyberprzestępczości, jest kluczowe dla późniejszych rozwiązań rachunkowości. Celem artykułu jest wyjaśnienie i analiza problemów rachunkowości związanych z kosztami cyberprzestępczości, w szczególności:

- dokonanie klasyfikacji kosztów cyberprzestępczości, przydatnej z punktu widzenia rachunkowości,
- omówienie zasad ujmowania kosztów cyberprzestępczości w księgach rachunkowych,
- analiza problemów zarządzania kosztami cyberprzestępczości, w szczególności opracowanie etapów wdrożenia procesu zarządzania zmianą w odniesieniu do kosztów cyberprzestępczości.

W wyniku podjętych rozważań zidentyfikowano koszty cyberprzestępczości w klasyfikacji rodzajowej i procesowej, dostosowane do warunków rachunku kosztów działań, który można zastosować do analizy i zarządzania tymi kosztami. Ponadto artykuł porusza problemy rachunkowości zarządczej, związanej z kosztami cyberprzestępczości oraz zarządzania ryzykiem operacyjnym. Zaproponowano schemat (etapy) wdrożenia procesu zarządzania zmianą w odniesieniu do kosztów cyberprzestępczości, posiłkując się zintegrowanym podejściem do zarządzania zmianą, obejmującym nurt systemowy i behawioralny. Metodami badawczymi

są analiza literatury oraz badania ankietowe. Posłużono się także techniką zwaną rejestr cech (ang. *selective listing*, *atribute listing*), zaliczaną jako odmiana techniki Gordona.

Słowa kluczowe: cyberkoszty, koszty cyberprzestępczości, zarządzanie ryzykiem cyberprzestępczości
Kod klasyfikacji JEL: M

1. Wprowadzenie

Koszty cyberprzestępczości to te z kosztów, które zaistniały w cyberprzestrzeni albo powstały w podmiocie gospodarczym w związku z jej istnieniem. Cyberprzestrzeń jest pojęciem definiowanym w dokumentach, opracowaniach naukowych, beletrystyce i regulacjach prawnych, co zostało podsumowane w tabeli 1.

Do pojęć bliskoznacznych, czasem stosowanych zamiennie do cyberprzestrzeni, należą przestrzeń wirtualna, świat wirtualny, rzeczywistość elektroniczna, świat cyfrowy, świat elektroniczny czy nawet wirtualizacja rzeczywistości. Wszystkie z tych zjawisk są tworzone przez człowieka, bo to przecież człowiek tworzy rzeczywistość, czasami nieświadomie. Ponadto charakteryzuje je pewna abstrakcja i potencjalizacja (zgodnie ze *Słownikiem wyrazów obcych* W. Kopalińskiego, „wirtualny" oznacza możliwy, mogący zaistnieć[1]), charakterystyczna dla współczesności, co można poprzeć stwierdzeniem wybitnego polskiego psychiatry A. Kępińskiego, który napisał, że człowiek, aby przetrwać, musi pogodzić dwie przeciwstawne postawy: kosmonauty i artysty[2]. Kosmonauta oczywiście w znaczeniu gotowości i otwartości na nowe we wszechświecie, artysta w kontekście opisu.

Istnieją także poglądy, że rzeczywistość wirtualna to ta, w której właśnie funkcjonujemy, której złożoności do końca jeszcze nie poznaliśmy, którą badają odrębnie różne dyscypliny nauki, takie jak fizyka, chemia, nauki biologiczne i inne, z każdym nowym odkryciem ujawnia się jej piękno i nie przestaje zaskakiwać. Niektórzy za Z. Baumanem uważają, że: „pojęcia, którymi się posługujemy, ukształtowały się w warunkach, które już nie istnieją. Używanie ich ma charakter metaforyczny.

[1] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Wydawnictwo Naukowe PWN, Warszawa 2000.

[2] M. Berdel-Dudzińska, *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, http://www.aplikanci.profinfo.pl/gfx/lexisnexis/userfiles/files/Pojecie-cyberprzestrzeni-we-wspolczesnym-polskim-porzadku-prawnym.pdf, dostęp 11.11.2016.

Staramy się uchwycić nowe zjawiska, wtłaczając je w stare ramy"[3]. Bauman wyraża również pogląd, że z socjologicznego punktu widzenia przestrzeń wirtualna jest potężnym narzędziem uniezależniania się nowej globalnej władzy od lokalnych, fizycznych ograniczeń.

Tabela 1. Definicje cyberprzestrzeni

Lp.	Źródło	Definicja
1	W. Gibson, *Burning Chrome*, *Neuromancer*	„Konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych (…) Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność… świetlne linie przebiegały bezprzestrzeń umysłu, skupiska i konstelacje danych"*
2	Komisja Europejska, *Słownik pojęć z zakresu społeczeństwa informacyjnego***	Wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata
3	Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej****	Przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami
4	*Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011–2016*****	Cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Cyberprzestrzeń RP – cyberprzestrzeń w obrębie terytoriom państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)

* Fragment książki w tłumaczeniu P. Cholewy. W. Gibson, *Neuromancer*, Katowice 2009, Książnica, s. 59; cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-fad9287e-d6f2-4713-ad9e-472717378ab4/c/Janusz_Wasilewski.pdf

** Komisja Europejska, *Słownik pojęć z zakresu społeczeństwa informacyjnego*; cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, File:///D:/dokument/Downloads/janusz%20Wasilewski%20(1).pdf, dostęp 11.11.2016.

*** Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej*, Warszawa 2013. File://D:/dokument/Downloads/POlityka_Ochrony_Cyberprzestrzeni_RP_148x210_wersja_pl.pdf, dostęp 11.11.2016.

**** Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011–2016, Warszawa 2010, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf

Źródło: opracowanie własne.

[3] *Globalizacja-proces nieodwracalny, rozmowa z prof. Z Baumanem z Leeds University*, http://www.panol.lublin.pl/biul_6/art_610.htm, z lipca 2011, cyt za: http://www.aplikanci.profinfo.pl/gfx/lexisnexis/userfiles/files/Pojecie-cyberprzestrzeni-we-wspolczesnym-polskim-porzadku-prawnym.pdf, dostęp 11.11.2016.

Ponieważ w rachunkowości nie zdefiniowano jednoznacznie pojęcia cyberprzestrzeni, na potrzeby niniejszego opracowania przyjmuje się założenie, że cyberprzestrzeń będzie miała zasięg podmiotowy (metoda podmiotowa jest przyjęta w rachunkowości za obowiązującą, dlatego na potrzeby niniejszego opracowania zawężono zasięg cyberprzestrzeni do podmiotu) i w tym kontekście będzie to cyfrowa przestrzeń danego pomiotu gospodarczego do przetwarzania, prezentowania i wymiany informacji z innymi użytkownikami. Cyberprzestrzeń jest zatem wytworem przedsiębiorstwa, charakteryzuje ją rozległość, złożoność, różnorodność baz danych, zróżnicowany dostęp do danych jej poszczególnych użytkowników (głównie pracowników, ale również użytkowników zewnętrznych) oraz różnorodne powiązania między użytkownikami. Koszty cyberprzestępczości, które są przedmiotem analizy niniejszego opracowania, będą wynikać z funkcjonowania cyberprzestrzeni w podmiocie gospodarczym i poza nim. Analiza zjawiska prowadzona będzie z uwzględnieniem rachunkowości finansowej oraz elementów rachunkowości zarządczej.

2. Uzasadnienie wyboru tematu

Cyberataki i tego typu zagrożenia to coraz popularniejsza forma przestępczości, pochłaniająca coraz więcej środków pieniężnych na działania prewencyjne i usuwanie szkód oraz coraz więcej kosztów podmiotów gospodarczych. Według raportu PWC głównym celem ataków są spółki świadczące usługi finansowe[4], ale zagrożenie dotyczy każdego podmiotu gospodarczego oraz osoby fizycznej.

W Australii ataki dotknęły głównie linii lotniczych, sieci hoteli i firm z sektora usług finansowych. Z raportu CSIS prowadzonego w 2013 r. w Stanach Zjednoczonych wynika, że 3 tysiące firm otrzymało od rządu powiadomienie o ataku hakerskim; większość tych podmiotów prowadzi sprzedaż detaliczną. W Wielkiej Brytanii koszty cyberprzestępstw w tej branży wyniosły 850 mln dolarów[5].

Ponemon Institute podjął próbę oszacowania kosztów, które ponoszą podmioty gospodarcze, będące ofiarami cyberataków. Zgodnie z ich raportem wyciek danych to dla podmiotu koszt bezpośredni średnio 65 euro związany z usunięciem

[4] PWC, *Zarządzanie ryzykiem w cyberprzestrzeni. Kluczowe obserwacje z wyników ankiety „globalny stan bezpieczeństwa informacji 2015"*, www.pwc.pl/bezpieczenstwo-biznesu, dostęp 11.11.2016.

[5] A. Ścibor, *Przeciwdziłanie cyberprzestępczości – raport McAfee i Centrum CSIS*, https://avlab.pl/przeciwdzialanie-cyberprzestepczosci-raport-mcafee-i-centrum-csis, dostęp 11.11.2016.

zagrożenia i jego efektów oraz 125 euro kosztów pośrednich. Koszty ponoszone po wykradnięciu danych, tj. praca helpdesków, wewnętrznych zespołów śledczych, komunikacja wewnętrzna to ponad 1 400 000 euro. Koszty związane z wykrywaniem i eskalacją (audyt, zarządzanie kryzysowe, postępowania sądowe) – ponad 500 000 euro[6]. Powyższe fakty świadczą o narastającym problemie powstawania kosztów cyberprzestępczości oraz przenoszeniu przestępczości do cyberprzestrzeni. Według prognoz firmy analitycznej Cybersecurity Ventures liczba danych, które będą musiały zostać objęte cyberochroną, wzrośnie pięćdziesięciokrotnie. Koszty cyberprzestępczości wzrosną z 3 bln dolarów w 2016 r. do 6 bln dolarów w 2021 r.[7]. Szacuje się, że koszty cyberprzestępczości w 2013 r. w USA wynosiły 38 mld USD, w Europie 12 mld USD; 38% spośród nich to następstwa oszustw[8].

W celu potwierdzenia istotności podejmowanych rozważań, w 2017 r. autorka podjęła się zbadania 50 studentów Uniwersytetu Ekonomicznego w Katowicach. Spośród osób objętych badaniem prawie 90% zetknęło się z cyberprzestępczością, 30% poniosło osobiście koszty, wynikające z przestępstw w cyberprzestrzeni, 100% ankietowanych uważa problem cyberprzestępczości za istotny, prawie 60% ankietowanych obawia się zagrożeń w cyberprzestrzeni.

Według raportu Center for Strategic and International Studies (CSIS) zatytułowanego „Net Losses – Estimating the Global Cost of Cybercrime" cyberprzestępczość wpływa negatywnie na innowacje, krajowe rynki, handel, konkurencyjność oraz wzrost gospodarczy. Szczególną szkodę wyrządza własności intelektualnej[9].

Na świecie podejmowane są różnorodne inicjatywy na rzecz zwiększenia bezpieczeństwa w sieci. W Polsce od 2008 r. powołany został CERT.GOV.PL (ang. Computer Emergency Response Team) – Rządowy Zespół Reagowania na Incydenty Komputerowe, którego zadaniem jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami[10].

---

[6] *Bezpieczeństwo danych: jak nie dać się cyberprzestępcy?*, http://www.egospodarka.pl/127088, Bezpieczenstwo-danych-jak-nie-dac-się-cyberprzestepcy,1,12,1.html, dostęp 11.11.2016.

[7] M. Duszczyk, *Koszty cyberprzestępczości podwoją się do 2021 roku*, http://www.rp.pl/Telekomunikacja-i-IT/309309935-Koszty-cyberprzestępczości-podwoja-sie-do-2021-roku.html, dostęp 11.11.2016.

[8] M. Czyżak, *Cyberprzestępczość a rozwój społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2015, nr 117, s. 665–673.

[9] J. Michalczyk, *Koszty cyberprzestępczości*, http://www.it-professional.pl/archiwum/art,5047, koszty-cyberprzestepczosci.html, dostęp 11.11.2016.

[10] J. Żuk, M. Żuk, *Zagrożenie w cyberprzestrzeni a bezpieczeństwo jednostki*, „Rozprawy społeczne" 2016, t. 10, nr 3, s. 71–77.

Powyższe informacje potwierdzają wagę i istotność problemów cyberprzestępczości. W odniesieniu do rachunkowości przedsiębiorstw te kwestie nie stały się jeszcze przedmiotem regulacji prawnych, praktyka podmiotów gospodarczych sprowadza się najczęściej do standardowego ujęcia kosztów *ex post* albo ujmowania programów typu *security*. Dodatkowym argumentem przemawiającym za poparciem wszechstronnych inicjatyw, wobec których rachunkowość się nie izoluje (o czym świadczy podjęcie takiego odważnego tematu na Forum Rachunkowości), jest dążenie autorki do wszechstronności podejmowanych w rachunkowości problemów informacyjnych, zgodnie z postawą opisaną przez K. Dąbrowskiego. Dąbrowski, w książce zatytułowanej „Trud istnienia" twierdzi, że w wielu naukach empirycznych o wyodrębnionym zakresie i określonych metodach badawczych spotykamy dwa odrębne typy postaw uczonych. Jedni, dążąc do głębszego rozumienia zasadniczych problemów nauki, szukają rozwiązań zarówno w wąskim zakresie danej dyscypliny, jak i poza nim; drudzy, aby zachować niezależność swoich metod, aby się „nie rozpraszać" nie wychodzą poza zakres swej specjalności[11].

3. Pojęcie kosztów cyberprzestępczości i ich ujęcie księgowe

Koszty cyberprzestępczości są związane z realizacją zagrożeń występujących w cyberprzestrzeni, które zostały opisane w literaturze przedmiotu. Najdokładniejszy katalog zagrożeń zawiera CERT.GOV.pl, który to zaprezentowano w tabeli 2.

Zdaniem autorki, dla rachunkowości przydatniejszy będzie przedstawiony poniżej podział kosztów cyberprzestępczości na cztery podstawowe grupy:

1) koszty związane z kradzieżą lub wyłudzeniem poufnych informacji, w celu ich wykorzystania na szkodę podmiotu gospodarczego; powinny być zaliczane do pozostałej działalności operacyjnej (inne pozostałe koszty operacyjne) i prezentowane w rachunku zysków i strat (sprawozdaniu z całkowitych dochodów) w wyniku z działalności operacyjnej;
2) koszty związane z niszczeniem, uszkodzeniem mienia oraz informacji – te również zaliczane powinny być do działalności pozostałej operacyjnej i prezentowane w rachunku zysków i strat (sprawozdaniu z całkowitych dochodów) w wyniku

[11] M. Berdel-Dudzińska, *Pojęcie*…, op.cit.

z działalności operacyjnej (nieplanowe odpisy umorzeniowe lub inne pozostałe koszty operacyjne);

3) koszty procesów sądowych związane z cyberprzestępczością – pozostałe koszty operacyjne lub rozwiązanie rezerwy / biernych rozliczeń międzyokresowych kosztów;
4) koszty podjętych działań ochraniających przed cyberprzestępczością – jeżeli dotyczą ochrony przed ryzykiem operacyjnym, to koszty podstawowej działalności operacyjnej, w szczególnych przypadkach mogą być również w formie czynnych rozliczeń międzyokresowych kosztów.

Tabela 2. Katalog zagrożeń według CERT.GOV.pl

<table>
<tr><td colspan="2">Zagrożenia</td><td colspan="5">Podatności</td></tr>
<tr><td rowspan="8">Działania celowe</td><td>Oprogramowanie złośliwe</td><td>Wirus</td><td>Robak sieciowy</td><td>Koń trojański</td><td>Dialer</td><td>Klient botnetu</td></tr>
<tr><td>Przełamanie zabezpieczeń</td><td>Nieuprawnione logowanie</td><td colspan="2">Włamanie na konto / ataki sieciowe</td><td colspan="2">Włamanie do aplikacji</td></tr>
<tr><td>Publikacje w sieci internet</td><td>Treści obraźliwe</td><td>Pomawianie/ Zniesławienie</td><td colspan="2">Naruszenie praw autorskich</td><td>Dezinformacja</td></tr>
<tr><td>Gromadzenie informacji</td><td>Skanowanie</td><td>Podsłuch</td><td>Inżynieria społeczna</td><td>Szpiegostwo</td><td>SPAM</td></tr>
<tr><td rowspan="3">Sabotaż komputerowy</td><td colspan="2">Nieuprawniona zmiana informacji</td><td colspan="3">Nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji</td></tr>
<tr><td colspan="2">Atak odmowy dostępu (np. DDoS, DOS)</td><td colspan="3">Skasowanie danych</td></tr>
<tr><td colspan="2">Wykorzystanie podatności w urządzeniach</td><td colspan="3">Wykorzystanie podatności aplikacji</td></tr>
<tr><td>Czynnik ludzki</td><td colspan="2">Naruszenie procedur bezpieczeństwa</td><td colspan="3">Naruszenie obowiązujących przepisów prawnych</td></tr>
<tr><td>Cyberterroryzm</td><td colspan="5">Przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni</td></tr>
<tr><td rowspan="2">Działania niecelowe</td><td>Wypadki i zdarzenia losowe</td><td>Awarie sprzętowe</td><td>Awarie łącza</td><td colspan="3">Awarie (błędy oprogramowania)</td></tr>
<tr><td>Czynnik ludzki</td><td>Naruszenie procedur</td><td>Zaniedbanie</td><td>Błędna konfiguracja urządzenia</td><td>Brak wiedzy</td><td>Naruszenie praw autorskich</td></tr>
</table>

Źródło: http://www.cert.gov.pl

Koszty związane z kradzieżą lub wyłudzeniem poufnych informacji, w celu ich wykorzystania na szkodę podmiotu gospodarczego, to m.in.:

- kradzieże tożsamości, danych pracownika,
- incydenty obraźliwych i nielegalnych treści dotyczące pracowników lub podmiotu gospodarczego,
- przełamanie zabezpieczeń dostępu wewnątrz systemu,
- ataki socjotechniczne, np. phishing, wyłudzanie informacji przez podszywanie się pod osobę godną zaufania albo fikcyjną instytucję i oszustwa z tym związane,
- hacking komputerowy – ominięcie zabezpieczeń systemowych i uzyskanie nieautoryzowanego dostępu do informacji podmiotu gospodarczego,
- podsłuch komputerowy – nieuprawnione przechwycenie wszelkich informacji podmiotu gospodarczego, znajdujących się w cyberprzestrzeni.

Koszty związane z niszczeniem, uszkodzeniem mienia oraz informacji to m.in.:

- bezprawne niszczenie informacji, jej uszkadzanie, usuwanie lub zmiana treści informacji, np. ataki z użyciem szkodliwego oprogramowania wirusowego,
- niszczenie sprzętu i oprogramowania,
- wprowadzenie kodu złośliwego z sieci LAN lub WAN, które spowoduje np. brak aktualizacji oprogramowania,
- blokowanie dostępu do usług (mail bomb, DoS, DDoS),
- blokowanie dostępu do istotnych informacji, skierowanych do upoważnionych w podmiocie gospodarczym osób,
- zakłócenie automatycznego przetwarzania informacji,
- sabotaż komputerowy – zakłócenia lub paraliżowanie funkcjonowania systemu informacyjnego w podmiocie gospodarczym.

Określenie wartości wymienionych kosztów cyberprzestępczości nie jest prostym zadaniem. Niektóre z nich są oczywiste do oszacowania, np. koszty zniszczenia sprzętu elektronicznego lub oprogramowania, koszty utraconych zasobów pieniężnych – w wartości wynikającej z ksiąg rachunkowych, koszty procesów sądowych – w wartości nominalnej. Inne koszty cyberprzestępczości należy szacować racjonalnie, są to np. koszty blokowanych dostępów do usług, zakłócenia w przetwarzaniu informacji i inne – tu wyraźnie musi być oszacowana szkoda, która powstała w wyniku cyberprzestępczości, często są to koszty zasądzone w drodze sądowej lub przyjęte w ramach zadośćuczynienia za szkodę – w sytuacji polubownego rozwiązania sporu.

Warto zaznaczyć, że na koszty związane z cyberprzestępczością powinna być, zdaniem autorki, tworzona rezerwa, bierne rozliczenia międzyokresowe kosztów

(gdy prawdopodobieństwo zaistnienia kosztów jest większe), ewentualnie czynne rozliczenia międzyokresowe kosztów w przypadku poniesionych kosztów ochrony przed cyberprzestępczością, choć nie ma wyraźnych wskazań w tym zakresie w regulacjach rachunkowości. Podobnie jak nie ma wskazania tej grupy kosztów w wyliczanych w ustawie o rachunkowości pozycjach pozostałych kosztów operacyjnych, choć są wyliczone koszty dochodzone na drodze sądowej.

4. Koszty cyberprzestępczości jako element zarządzania

Rozpatrując funkcjonalną systematykę kosztów cyberprzestępczości, dostosowaną do potrzeb zarządzania procesowego, należy rozróżnić dwie podstawowe grupy kosztów, związane z wykonywanymi procesami ochronnymi i zarządczymi. Pierwszą grupę stanowią koszty zapobiegania cyberatakom i ochrony przed nimi, powstające na skutek podejmowania takich właśnie procesów, które zaliczyć można do procesu zarządzania ryzykiem operacyjnym. Drugą grupę kosztów funkcjonalnych stanowią koszty zarządzania, głównie zarządzania zmianą lub przez zmianę, związane identyfikacją i usuwaniem skutków cyberataków.

Koszty identyfikacji i usuwania skutków cyberataków to w szczególności narzędzia i systemy do wykrywania włamań, przechowywania danych o użytkownikach oraz monitorowania ich zachowań, narzędzia wykrywania włamań, złośliwych kodów i innych zagrożeń, koszty likwidacji konsekwencji cyberataku oraz doprowadzenia cyberprzestrzeni przedsiębiorstwa do stanu bezpiecznego. Są to pozycje kosztów odpowiadające zadaniom zarządczym, a więc związane z zachodzącymi procesami, wprowadzanymi w życie zarówno przed cyberatakiem, jak i *ex post*. Na wyróżnienie w tej grupie zasługują koszty ubezpieczeń od następstw cyberataków, które stają się coraz popularniejsze, zwłaszcza w podmiotach finansowych, z sektora telekomunikacyjnego i produkcji przemysłowej i które mają stanowić element strategii zarządzania ryzykiem. W Stanach Zjednoczonych SEC OCIE wydał wytyczne, aby podmioty z sektora finansowego zawierały ubezpieczenia przed cyberyzykiem[12]. Podejmowane aktywności z zakresu rachunkowości zarządczej, generujące koszty tej grupy, to działania legislacyjno-regulujące w postaci tworzenia instrukcji i zarządzeń, działania proceduralno-organizacyjne, edukacyjne oraz działania techniczne. Ze względu na stale zmieniające się zagrożenia i wymagania

[12] PWC, *Zarządzanie…*, op.cit.

biznesu, działania zarządcze często wyprowadzane są z modelu zarządzania zmianą lub zarządzania przez zmianę, procesu który łączy ze sobą elementy składowe teorii zarządzania, metod i technik organizowania oraz wiedzy socjologicznej, psychologicznej, ekonomicznej i technicznej[13]. Należy jednak pamiętać, że zmianami nie da się w pełny sposób zarządzać, można je jedynie wyprzedzać, antycypować oraz naprawiać konsekwencje[14]. Dlatego centralne miejsce w ochronie przed cyberatakami mają działania z zakresu zarządzania ryzykiem, z którymi związana jest kolejna grupa kosztów cyberprzestępczości z systematyki funkcjonalnej.

Koszty zapobiegania i ochrony przed ryzykiem to grupa kosztów ponoszonych *ex ante*, przed potencjalnym cyberatakiem; stanowi ukoronowanie działań zarządczych związanych z cyberprzestępczością. Zaliczamy do nich m.in. koszty szkoleń pracowników, koszty zabezpieczeń kontroli dostępu, koszty wprowadzania instrumentów zapobiegających przed cyberatakami, takich jak szyfrowanie wiadomości e-mail, systemy zapobiegania włamaniom i utracie danych oraz niszczeniu sprzętu elektronicznego i oprogramowania. W ustanowieniu własnej procedury w tym zakresie można posiłkować się m.in. *Metodyką zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych*[15]. Zgodnie z tym dokumentem zarządzanie ryzykiem cyberprzestrzeni odbywa się według modelu przedstawionego na rysunku 1.

W procedurze zarządzania ryzykiem rozróżniamy przedstawione niżej elementy[16].

1. Identyfikowanie ryzyka w poszczególnych kategoriach zagrożeń.
2. Analiza ryzyka, na którą składają się:
   - szacowanie następstw,
   - szacowanie prawdopodobieństwa incydentu,
   - określenie poziomu ryzyka.
3. Ocena ryzyka, polegająca na porównaniu wyznaczonych poziomów ryzyka z ryzykiem akceptowalnym przyjętym dla danej kategorii aktywności.

---

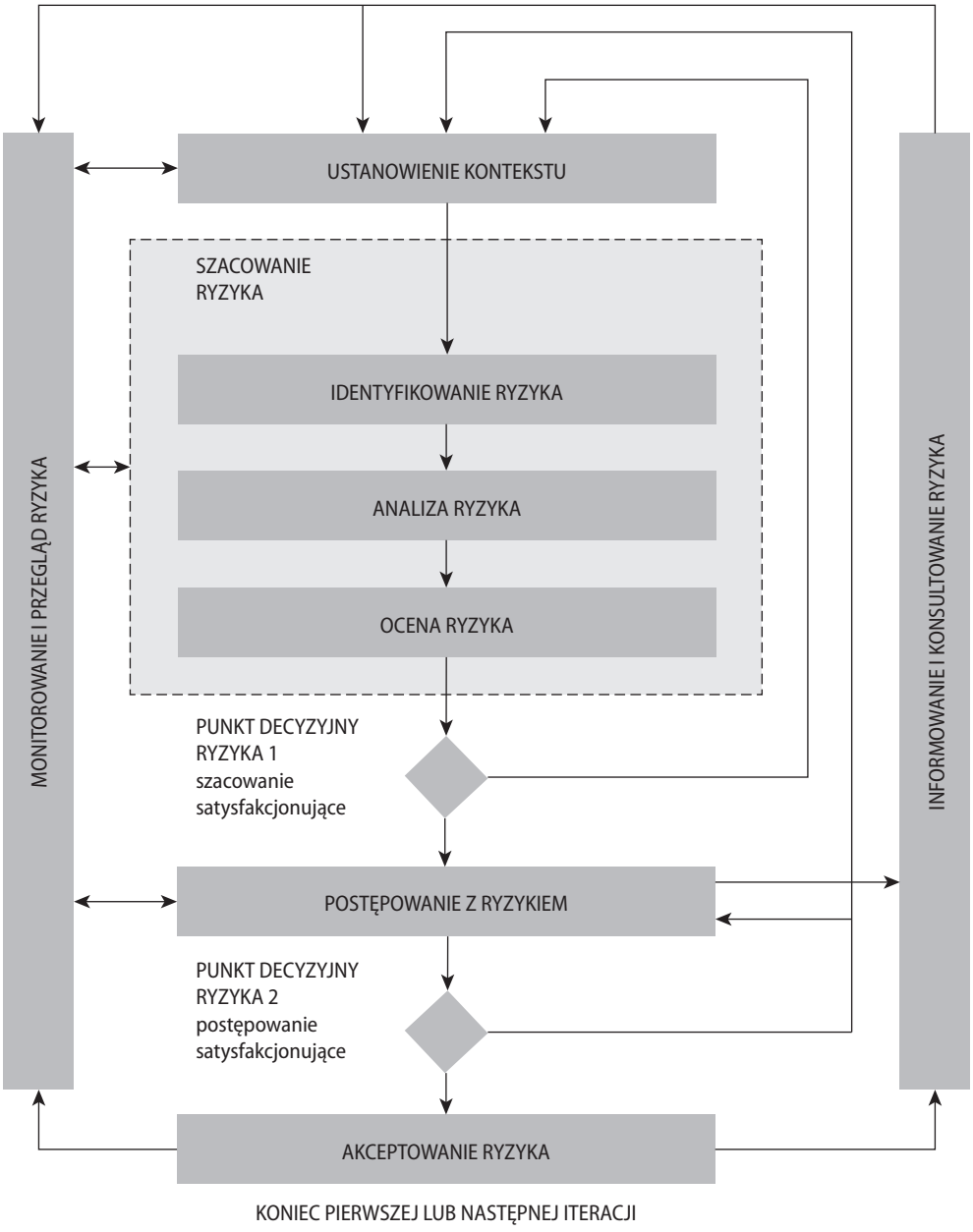
[13] M. Bratnicki, *Zarządzanie zmianami w przedsiębiorstwie*, Wydawnictwo A.E. w Katowicach, Katowice 1998, s. 9.

[14] P.F. Drucker, *Zarządzanie XXI wieku – wyzwania*, Wydawnictwo MT Biznes, Warszawa 2009, s. 83.

[15] *Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych*, Warszawa 2015, Krmc.mc.gov.pl/…/MetodykaZarządzaniaRyzykiemCRP2015v18ZZKR

[16] Ibidem.

Rysunek 1. Model zarządzania ryzykiem cyberprzestępczości



Źródło: *Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych*, Krmc.mc.gov.pl/…/MetodykaZarządzaniaRyzykiemCRP2015v18ZZKR

4. Postępowanie z ryzykiem, które może polegać na:
   – zastosowaniu zabezpieczenia,
   – unikaniu ryzyka,
   – przeniesieniu ryzyka,
   – akceptacji ryzyka.
5. Informowanie o ryzyku – rejestry ryzyka, raporty.
6. Dokumenty i zapisy.
7. Raportowanie i terminy działań w zarządzaniu ryzykiem.

Rządy wielu państw podejmują działania informujące i zabezpieczające, polegające na gromadzeniu i publikowaniu danych dotyczących cyberprzestępczości, informują o możliwościach ochrony, formułują własną politykę cyberprzestrzeni oraz metodyki zarządzania ryzykiem cyberprzestępczości. Przedsiębiorstwa korzystające z rządowej ochrony cyberprzestrzeni najczęściej stosują w ramach narzędzi zarządzania ubezpieczenie lub ochronę ze strony specjalistycznej firmy przed cyberatakami, samodzielnie zaś najczęściej stosują strategię koncentracji na najbardziej wartościowych aktywach oraz największych dla nich zagrożeniach. Wśród respondentów badania przeprowadzonego przez PWC 80% deklaruje, że polityka bezpieczeństwa spółki jest dobrze dostosowana do celów biznesowych. W Polsce klasyfikację wartości biznesowej danych dokonuje 36% badanych, 60% badanych przeprowadziło jakąś formę zarządzania aktywami, 34% respondentów badania PWC nie kieruje wydatków na bezpieczeństwo do najbardziej zyskownych pionów działalności. Do tego należy dodać, że światowe wydatki na bezpieczeństwo w ostatnich kilku latach nie przekroczyły 4% całego budżetu przeznaczonego na informatykę[17].

Najbardziej pasującym procesem zarządczym związanym z cyberprzestępczością jest proces zarządzania zmianą, który dzięki złożoności oraz etapowości w czasie, zmierza w ogólnym rozrachunku do osiągnięcia postawionego na początku celu ogólnego. Wskazaniem do wprowadzenia zmian jest zarówno otoczenie, względem którego przedsiębiorstwo powinno mieć określoną politykę działania, jak i przedsiębiorstwo, w którym każdy potencjalnie jest obciążony zmianą. Pierwszym krokiem jest przygotowanie ludzi i przedsiębiorstwa do zmian, drugim krokiem jest sama zmiana, trzecim – konsolidacja zmian w systemie[18]. Istnieje wiele propozycji autorów w zakresie faz (etapów) zarządzania zmianą. W opracowaniu posiłkowano

[17] PWC, *Zarządzanie*…, op.cit.

[18] J. Furman, M. Kuczyńska-Chałada, *Change Management in Lean Enterprise*, „Economics and Management" 2016, nr 2, s. 24–31.

się propozycją R. Wendta[19], którą dostosowano do zarządzania kosztami cyberprzestępczości. Należy także zaznaczyć, że zmiana może być dokonywana *ex post*, po zaistnieniu incydentu w cyberprzestrzeni oraz usunięciu jego skutków, ale może być również przeprowadzona *ex ante*, w drodze partycypacji potencjalnych zagrożeń. Oba sposoby wprowadzania zmian mają charakter udoskonalający metodykę postępowania z cyberprzestępczością, jednak ponieważ zalecany i preferowany jest sposób drugi, ten zostanie poddany dalszemu wyjaśnieniu. W rozpatrywaniu tego zagadnienia stosować należy nurt zintegrowany zarządzania zmianą, łączący w sobie elementy nurtu systemowego oraz behawioralnego[20].

Proponuje się następujące etapy (fazy) procesu zarządzania zmianą w odniesieniu do kosztów cyberprzestępczości:

1) określenie krytycznych elementów struktury cyberprzestrzeni (nurt systemowy) oraz zachowań pracowniczych (nurt behawioralny), wystawionych na ryzyko operacyjne związane z kosztami cyberprzestępczości[21];
2) określenie stopnia zagrożenia kosztami cyberprzestępczości i decyzja o podjęciu lub nie działań ochronnych przed cyberprzestępczością – metody wykorzystane w szacunkach ryzyka operacyjnego;
3) przygotowanie się do wdrożenia zmiany; etap ten obejmuje projektowanie zmian, analizę krytycznych elementów cyberprzestrzeni od kątem reakcji na zmianę – w warunkach cyberataku, monitorowanie zachowań pracowniczych i ich przekonania do zmiany; zmiana najczęściej obejmuje wprowadzenie działań prewencyjnych i monitorujących w krytycznych elementach strukturalnych, celem odstraszenia potencjalnych cyberprzestępców, badanie funkcjonowania kodów dostępu, destabilizację *status quo* i przeszkolenie pracowników z zakresie pożądanych zachowań, badanie możliwości i kosztów podjęcia środków ochronnych oraz reakcji w sytuacji zagrożenia cyberatakiem, a także wybór właściwego momentu i oczekiwanie na realizację zmiany;
4) realizacja zmiany; wprowadzenie projektowanych instrumentów w życie;
5) wzmocnienie wdrożonych zmian;

[19] R. Wendt, *Zarządzanie zmianą w polskiej firmie*, Dom Wydawniczy Zachorek, Warszawa 2010, s. 41–82.

[20] A. Zarębska, *Zmiany organizacyjne w przedsiębiorstwie. Teoria i praktyka*, Difin, Warszawa 2002, s. 35–73.

[21] A. Sujova, K. Marcinekova, *The Assignment of Starting Points within Management of Change*, „Zeszyty Naukowe Wyższej Szkoły Humanitas: Zarządzanie" 2016, nr 4, s. 367–376.

6) synchronizacja i kompatybilność działań między poszczególnymi obszarami, w rachunkowości właściwe informacje zwrotne, pozwalające dostosować poziom rezerw do rzeczywistego zagrożenia cyberatakiem.

Zaznaczyć należy, że proces zarządzania zmianą należy projektować w szczegółach wciąż na nowo, dostosowując się do wykonywanych aktywności w cyberprzestrzeni oraz przedsięwziętych instrumentów. Trzymanie się proponowanego schematu ułatwia wdrożenie zmiany i pozwala na zachowanie powtarzalności zadań w warunkach zmienności.

5. Podsumowanie

Koszty cyberprzestępczości oraz zarządzanie ryzykiem cyberprzestępczości stanowią nową kategorię w systemie rachunkowości w zakresie jej ujmowania i sprawozdawania, jak również jako istotnej kategorii zarządzania, zwłaszcza w odniesieniu do zarządzania ryzykiem. Ze względu na dość dużą i rosnącą częstotliwość takich incydentów oraz istotne konsekwencje ekonomiczne i finansowe cyberataków, nakłady na eliminację tego typu zagrożeń mogą stać się interesującą kategorią sprawozdawczą, zwłaszcza dla potencjalnych kontrahentów, nawiązujących współpracę z podmiotem gospodarczym. Jak wskazują badania PWC, ataki koncentrują się zwłaszcza na podmiotach finansowych, liniach lotniczych oraz przedsiębiorstwach przemysłowych (a więc podmiotach, z którymi większość łączą jakieś stosunki handlowe); często są to także małe spółki, które mają pełnić funkcję przyczółka do wejścia przez nie do innych podmiotów[22]. W artykule przedstawiono systematykę rodzajową oraz funkcjonalną kosztów cyberprzestępczości, zasady ich ujmowania w księgach rachunkowych i skutki sprawozdawcze. Poruszono także problematykę zarządzania tymi kosztami.

Bibliografia

Wydawnictwa zwarte

1. Bratnicki M., *Zarządzanie zmianami w przedsiębiorstwie*, Wydawnictwo A.E. w Katowicach, Katowice 1998.

[22] PWC, *Zarządzanie…*, op.cit.

2. Drucker P.F., *Zarządzanie XXI wieku – wyzwania*, Wydawnictwo MT Biznes, Warszawa 2009.
3. Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Wydawnictwo Naukowe PWN, Warszawa 2000.
4. Wendt R., *Zarządzanie zmianą w polskiej firmie*, Dom Wydawniczy Zachorek, Warszawa 2010.
5. Zarębska A., *Zmiany organizacyjne w przedsiębiorstwie. Teoria i praktyka*, Difin, Warszawa 2002.

Artykuły naukowe

1. Czyżak M., *Cyberprzestępczość a rozwój społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług" 2015, nr 117.
2. Furman J., Kuczyńska-Chałada M., *Change Management in Lean Enterprise*, „Economics and Mangement" 2016, nr 2.
3. Sujova A., Marcinekova K, *The Assignment of Starting Points within Management of Change*, „Zeszyty Naukowe Wyższej Szkoły Humanitas: Zarządzanie" 2016, nr 4.
4. Żuk J., Żuk M., *Zagrożenie w cyberprzestrzeni a bezpieczeństwo jednostki*, „Rozprawy społeczne" 2016, t. 10, nr 3.

Materiały internetowe

1. Berdel-Dudzińska M., *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, http://www.aplikanci.profinfo.pl/gfx/lexisnexis/userfiles/files/Pojecie-cyberprzestrzeni-we-wspolczesnym-polskim-porzadku-prawnym.pdf
2. *Bezpieczeństwo danych: jak nie dać się cyberprzestępcy?*, http://www.egospodarka.pl/127088, Bezpieczenstwo-danych-jak-nie-dac-się-cyberprzestepcy,1,12,1.html
3. Duszczyk M., *Koszty cyberprzestępczości podwoją się do 2021 roku*, http://www.rp.pl/Telekomunikacja-i-IT/309309935-Koszty-cyberprzestępczości-podwoja-sie--do-2021-roku.html
4. Gibson W, *Neuromancer*, tłumacz fragmentu P. Cholewa, Katowice 2009, Książnica, s. 59, cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-fad9287e-d6f^2-4713-ad9e--472717378ab4/c/Janusz_Wasilewski.pdf
5. *Globalizacja – proces nieodwracalny, rozmowa z prof. Z Baumanem z Leeds University*, http://www.panol.lublin.pl/biul_6/art_610.htm, z lipca 2011, cyt. za: http://www.aplikanci.profinfo.pl/gfx/lexisnexis/userfiles/files/Pojecie-cyberprzestrzeni--we-wspolczesnym-polskim-porzadku-prawnym.pdf.
6. http://www.cert.gov.pl.

7. Komisja Europejska, *Słownik pojęć z zakresu społeczeństwa informacyjnego*, cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, File:///D:/dokument/Downloads/janusz%20Wasilewski%20(1).pdf
8. *Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych*, Warszawa 2015, Krmc.mc.gov.pl/…/MetodykaZarządzaniaRyzykiemCRP2015v18ZZKR
9. Michalczyk J., *Koszty cyberprzestępczości*, http://www.it-professional.pl/archiwum/art,5047, koszty-cyberprzestepczosci.html
10. Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej*, Warszawa 2013, File://D:/dokument/Downloads/POlityka_Ochrony_Cyberprzestrzeni_RP_148x210_wersja_pl.pdf
11. PWC, *Zarządzanie ryzykiem w cyberprzestrzeni. Kluczowe obserwacje z wyników ankiety „globalny stan bezpieczeństwa informacji 2015"*, www.pwc.pl/bezpieczenstwo-biznesu
12. *Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011–2016*, Warszawa 2010, https://www.enisa.europa.eu/topics/national-cyber-security--strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf
13. Ścibor A., *Przeciwdziłanie cyberprzestępczości – raport McAfee i Centrum CSIS*, https://avlab.pl/przeciwdzialanie-cyberprzestepczosci-raport-mcafee-i-centrum-csis

Costs of Cybercrime. Accounting Prospects

Summary

Due to the growing informatisation of different aspects of corporate operation, it is crucial for the future accounting solutions to determine precisely what cybercrime and cybercrime costs are. The article is aimed at the explanation and analysis of accounting problems related to cybercrime, in particular:
– classification of cybercrime costs, useful from the accounting perspective,
– principles of presentation of cybercrime in account books,
– problems of cybercrime costs management, especially drawing up stages of implementation of the change management process in relation to cybercrime costs.
The undertaken study resulted in the identification of cybercrime costs in type and process classification, adjustable to the conditions of management of these costs. Furthermore, the article deals with the problems of managerial accounting connected with cybercrime costs and operational risk management. It presents a scheme (stages) of implementation of the

change management process related to cybercrime, based on the integrated approach to change management including a systemic and behavioural trend. The research method includes the literature analysis and surveys. Another technique used is attribute listing, a variation of the Gordon technique.

Keywords: cybercosts, cybercrime costs, cybercrime cost management

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 107–128

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

Magdalena Kludacz-Alessandri
Kolegium Nauk Ekonomicznych i Społecznych w Płocku
Politechnika Warszawska

Wpływ stopnia komputeryzacji szpitala na jakość kalkulacji kosztów świadczeń zdrowotnych

Streszczenie

Efektywna wycena procesu leczenia pacjenta wymaga szczegółowych informacji kosztowych pochodzących z systemu rachunkowości podmiotu leczniczego. Najważniejszym narzędziem wspomagającym system rachunkowości, a zwłaszcza proces kalkulacji kosztów świadczeń zdrowotnych, jest system informatyczny, który powinien być tak zaprojektowany, aby umożliwiać integrację danych finansowych i medycznych szpitala.

Celem artykułu jest analiza stopnia komputeryzacji szpitali i ocena wpływu tego czynnika na jakość rozwiązań w zakresie kalkulacji kosztów procesu leczenia pacjenta i stopień wykorzystania informacji kosztowych w procesie zarządzania szpitalem. Ocena ta została przeprowadzona na podstawie wyników badań empirycznych w szpitalach polskich, angielskich i słoweńskich. Na podstawie przeprowadzonej analizy literatury przedmiotu postawiono hipotezę badawczą, że czynnikiem, który w znacznym stopniu wpływa na jakość kalkulacji kosztów leczenia pacjenta i stopień wykorzystania informacji kosztowych w procesie zarządzania jest stopień zinformatyzowania szpitala. Do weryfikacji hipotez badawczych wykorzystano analizę korelacji i regresji wielorakiej. Przeprowadzone badania wykazały, że stopień komputeryzacji

szpitala jest czynnikiem, który w największym stopniu wpływa na jakość kalkulacji kosztów leczenia pacjenta, a ta z kolei – na stopień wykorzystania informacji kosztowych w procesie zarządzania szpitalem.

Słowa kluczowe: system informatyczny, rachunek kosztów, kalkulacja kosztów leczenia pacjenta
Kod klasyfikacji JEL: M41

1. Wprowadzenie

Do efektywnej wyceny świadczeń zdrowotnych potrzebne są informacje kosztowe, pochodzące z systemu rachunkowości podmiotu leczniczego. Konieczne jest przy tym takie zorganizowanie tego systemu, aby umożliwiał on przeprowadzenie kalkulacji kosztów jednostkowych różnych obiektów koniecznych do wyceny całego procesu leczenia pacjenta. Najważniejszym narzędziem wspomagającym system rachunkowości, a zwłaszcza proces kalkulacji kosztów świadczeń zdrowotnych, jest system informatyczny, który powinien być tak zaprojektowany, aby stosowane w nim rozwiązania były zgodne z wymaganiami ustawy o rachunkowości, a z drugiej strony umożliwiały integrację danych finansowych i medycznych szpitala.

Celem artykułu jest ocena stopnia komputeryzacji w wybranych szpitalach i jego wpływu na jakość kalkulacji świadczeń zdrowotnych, a także na stopień wykorzystania informacji kosztowych w procesie zarządzania. Podjęto zatem próbę odpowiedzi na następujące pytania badawcze:

- Jaki jest stopień komputeryzacji części medycznej i ekonomicznej badanych szpitali oraz stopień ich zintegrowania?
- Czy stopień komputeryzacji szpitala wpływa na jakość wyceny świadczeń zdrowotnych?
- Czy stopień komputeryzacji szpitala wpływa na zakres wykorzystania informacji kosztowych w procesie zarządzania szpitalem?

W artykule przedstawiono wyniki badania empirycznego przeprowadzonego w polskich, angielskich i słoweńskich szpitalach w latach 2012–2013. W badaniach uczestniczyli między innymi główni księgowi oraz kadra kierownicza szpitali.

2. Rachunkowość jako system informacyjny

Podnoszenie sprawności i skuteczność działania każdego podmiotu gospodarczego zależy od odpowiednio zorganizowanego i kompleksowego sytemu informacyjnego, którego kluczowym elementem jest system rachunkowości. Współcześnie rozumiana rachunkowość jest bardzo często definiowana właśnie jako system informacyjny podmiotu. Nawiązanie do systemu informacyjnego w kontekście rachunkowości pojawiło się po raz pierwszy na początku lat 70. XX w. w amerykańskiej literaturze przedmiotu w raporcie stowarzyszenia księgowych. System rachunkowości zdefiniowano wtedy jako podsystem funkcjonujący w ogólnych ramach systemów informacyjnych zarządzania, zajmujący się przetwarzaniem, przechowywaniem w czasie oraz raportowaniem informacji[1].

W polskiej literaturze przedmiotu podobne podejście do rachunkowości prezentował W. Brzezin, określając rachunkowość jako zinstytucjonalizowany podsystem systemu informacyjnego zarządzania, wspomagającego proces podejmowania decyzji ekonomicznych poprzez gromadzenie i przetwarzanie danych dotyczących majątku jednostki gospodarczej i jej działalności oraz prezentację informacji ekonomiczno-finansowej. Podsystem ten odzwierciedla realistycznie zdarzenia gospodarcze pomiędzy podmiotem a jego otoczeniem i przetwarza je w agregaty ujęte w wielkościach pieniężnych dla celów planowania, sterowania, nadzorowania i publikowania w podmiocie[2]. Przykładowe definicje rachunkowości jako systemu informacyjnego zaprezentowano w tabeli 1.

Tabela 1. Definicje rachunkowości jako systemu informacyjnego

Autor	Definicja
A. Jarugowa	System informacyjny służący użytkownikom do podejmowania decyzji gospodarczych, zwłaszcza finansowych oraz rozliczania kierownictwa z odpowiedzialnego i efektywnego zarządzania powierzonym majątkiem
K. Sawicki	Rachunkowość stanowi uniwersalny i elastyczny system informacyjny, umożliwiający prawidłowe i rzetelne przedstawianie zasobów, źródeł ich finansowania, przebiegu i warunków działalności przedsiębiorstwa oraz tworzenie podstaw oceny i podjęcia decyzji przez użytkowników informacji

[1] J. Turyna, *System informacyjny rachunkowości*, Wydawnictwa Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa 1997, s. 44–46.

[2] W. Brzezin, *Ogólna teoria rachunkowości*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 1995, s. 22.

Autor	Definicja
E. Burzym	Rachunkowość stanowi uniwersalny, elastyczny, podmiotowy system informacyjno-kontrolny, zdeterminowany metodą bilansową, która jest nierozerwalnie z nim związana i metodą poznawczą, umożliwiającą tworzenie liczbowego obrazu powstania, podziału i przepływu wartości oraz wynikających stąd rozrachunków między podmiotami gospodarczymi
B. Micherda	Rachunkowość jest uniwersalnym i elastycznym systemem informacyjno-kontrolnym, odzwierciedlającym przebieg i rezultaty działalności jednostek gospodarczych. Uniwersalność rachunkowości polega na możliwości dostosowania do specyficznych warunków działalności podmiotów, zdolności do jednoczesnego pełnienia różnych funkcji i zadań szczegółowych oraz przydatności do tworzenia liczbowego obrazu opartego na wielkościach rzeczywistych, jak też planowanych.

Źródło: opracowanie własne na podstawie: M. Król-Stępień, *System informatyczny rachunkowości jako narzędzie wspomagające zarządzanie jednostką gospodarczą – wymogi ustawowe, a ich praktyczne zastosowanie*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2013, nr 757, „Finanse, Rynki Finansowe, Ubezpieczenia" nr 58, s. 75–81; *Rachunkowość finansowa*, red. K. Sawicki, PWE, Warszawa 1999, s. 13–14; E. Burzym, *Rachunkowość przedsiębiorstw i instytucji*, PWE, Warszawa 1980, s. 13; B. Micherda, *Analityczna funkcja rachunkowości*, Wydawnictwo AE w Krakowie, Kraków 2001.

Z przedstawionych definicji wynika, że rachunkowość ma za zadanie dostarczać informacje, które będą pomocne dla ich odbiorców w ocenie zasobów podmiotu i jego działalności oraz w podejmowaniu racjonalnych decyzji. Informacje te powinny nie tylko umożliwiać ocenę jednostki, lecz także stwarzać podstawy efektywnego zarządzania. Celem systemu rachunkowości każdego podmiotu gospodarczego jest zatem dostarczenie rzetelnych informacji, umożliwiających ocenę jego sytuacji finansowej oraz podejmowanie decyzji ekonomicznych. Na system informacyjny rachunkowości składają się takie działania, jak: identyfikacja, grupowanie, opis, ewidencja, przetwarzanie i prezentowanie informacji finansowych podmiotu.

W literaturze przedmiotu podkreśla się zatem, że podstawową funkcją systemu rachunkowości jest funkcja informacyjna. Od współczesnej rachunkowości oczekuje się bowiem wiarygodnej i rzetelnej informacji, przedstawionej w jasny sposób w ujęciu retro- i prospektywnym. Istotnym elementem funkcji informacyjnej jest z kolei funkcja analityczna, która stanowi interpretację związków treściowych, które wynikają z przyczynowo-skutkowych uwarunkowań i przyjętych sposobów liczenia rachunkowości[3]. Przejawia się ona w badaniu i interpretacji zjawisk gospodarczych ujętych w systemie rachunkowości. Również inne definicje funkcji analitycznej rachunkowości wskazują na proces odpowiedniej interpretacji informacji

[3] B. Micherda, *Analityczna funkcja rachunkowości*, Wydawnictwo AE w Krakowie, Kraków 2001, s. 5.

pochodzących z rachunkowości[4]. Rezultatem analizy danych liczbowych generowanych w systemie rachunkowości są bowiem wnioski posiadające walory informacyjne, które pozwalają na ocenę działalności jednostki, efektywności wykorzystania zasobów i ujawnianie nieprawidłowości oraz stanowią podstawę podejmowanych decyzji zarządczych.

Informacje generowane w systemie rachunkowości szpitala powinny stanowić m.in. wsparcie w procesach kontraktowania świadczeń medycznych, kształtowania polityki cen usług medycznych oraz tworzyć warunki dokonywania oceny konsekwencji ekonomicznych wybranych procedur diagnozowania i leczenia. Potrzeby informacyjne zarządu szpitala dotyczą również kształtowania przychodów ze sprzedaży świadczeń medycznych, kosztów ich realizacji, właściwej alokacji zasobów wewnątrz szpitala, zabezpieczenia dostępności świadczeń, monitorowania przychodów i kosztów[5]. Rachunek kosztów jest zatem szczególnie istotnym elementem systemu rachunkowości szpitala, głównym źródłem informacji do podejmowania decyzji i narzędziem służącym do bieżącej kontroli kosztów usług medycznych.

3. System informatyczny jako narzędzie przetwarzania informacji kosztowych w systemie rachunkowości

Ważnym narzędziem do obsługi każdego systemu informacyjnego jest system informatyczny ukierunkowany na potrzeby konkretnych użytkowników, który powinien być tak zaprojektowany, aby stosowane w nim rozwiązania i procedury były zgodne z zasadami rachunkowości, pomagały jak najlepiej spełnić wymagania ustawowe stawiane księgom rachunkowym i jednocześnie usprawniały proces zarządzania[6]. Stanowi on zatem warunek konieczny do grupowania, ewidencji i przetwarzania informacji kosztowych na potrzeby wyceny świadczeń zdrowotnych. Intensywny rozwój technologii informatycznych sprawia, że trudno sobie wyobrazić podmioty lecznicze, które byłyby w stanie ręcznie przetwarzać niezliczoną ilość informacji

[4] K. Grabiński, *Analityczna funkcja rachunkowości w systemach informatycznych klasy ERP*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2005, nr 674, s. 103–112.

[5] M. Hass-Symotiuk, *Rachunkowość jako system generowania informacji ekonomiczno-finansowych na potrzeby zarządzania w zakładzie opieki zdrowotnej*, w: *Rachunkowość. System informacji finansowych Zakładów Opieki Zdrowotnej*, red. M. Hass-Symotiuk, Wolters Kluwer Polska, Warszawa 2010, s. 30.

[6] B. Kunz, A. Tymińska, *System informatyczny rachunkowości i jego rola w świetle ustawy o rachunkowości*, „Nauki o Finansach" 2014, 3, s. 44–58.

medycznych i ekonomicznych. Tym samym istotną rolę w procesie kalkulacji kosztów na potrzeby świadczeń zdrowotnych szpitali odgrywa stopień zinformatyzowania szpitala. Implementacja rachunku kosztów w środowisku informatycznym stwarza bowiem warunki do dokładniejszej kontroli kosztów oraz efektywniejszego zarządzania i dokładniejszej wyceny świadczeń zdrowotnych.

W praktyce podmiotów leczniczych mogą być stosowane różne systemy informatyczne, od najprostszych, wykorzystywanych jedynie do realizacji podstawowych funkcji finansowo-księgowych, po nowoczesne, zintegrowane systemy informatyczne, które wspierają proces zarządzania podmiotem leczniczym, gromadzą, przetwarzają oraz integrują różnorodne dane ekonomiczne i medyczne, dotyczące różnych obszarów funkcjonalnych. Mimo że komputery stanowią jedynie narzędzie wspomagające system rachunkowości szpitali, to sposób ich zastosowania w istotny sposób wpływa na jakość stosowanego rachunku kosztów i kalkulacji świadczeń zdrowotnych. Narzędzia komputerowo-informacyjne umożliwiają bowiem wielopłaszczyznową analizę kosztu całego procesu leczenia pacjenta, bez ponoszenia dodatkowych, znaczących nakładów czasowych i materialnych.

Standardowym rozwiązaniem powinno być zatem wdrożenie dostosowanego do potrzeb szpitala systemu wspomagającego rachunkowość, a nawet zintegrowanego systemu informatycznego zarządzania, tak jak to jest w przypadku większych przedsiębiorstw. Zintegrowany system informatyczny można zdefiniować jako wyodrębniony czasowo i przestrzennie układ przetwarzania danych oraz informacji, będący zbiorem celowo powiązanych ze sobą elementów, w którym wyróżnia się: źródła danych, środki materialne i ludzi, metody gromadzenia i przetwarzania danych, miejsca przeznaczenia informacji oraz kanały przepływu informacji. Podstawowym zadaniem zintegrowanego systemu informatycznego jest gromadzenie, przetwarzanie i dostarczanie decydentom w krótkim czasie terminowych i dokładnych informacji, pozwalających na usprawnienie procesu podejmowania niezbędnych decyzji i tworzenie ich zróżnicowanych wariantów z oceną możliwych skutków. Taki system może usprawnić rutynowe czynności, wykluczyć powtarzalność wprowadzania danych, efektywniej wykorzystać czas pracy pracowników i w skuteczny sposób osiągać wyznaczone przez podmiot cele[7].

Zintegrowany system informatyczny szpitala powinien mieć charakter kompleksowy i składać się z wielu różnych modułów, np. ruch chorych, rozliczenia

[7] B. Sadowska, *Znaczenie i warunki stosowania zintegrowanych systemów informatycznych w sferze budżetowej*, „Zeszyty Teoretyczne Rachunkowości" 2014, t. 76(132), s. 67.

pacjentów, dokumentacja medyczna, ambulatorium, statystyka medyczna. Szpitalne systemy informatyczne powinny być tak zaprojektowane, aby ułatwić zarządzanie nie tylko obszarami finansowymi, lecz także medycznymi. Takie systemy umożliwiają bowiem przetwarzanie danych związanych nie tylko z księgowością, lecz także z hospitalizacją pacjenta, gospodarką lekami, rozliczeniami z płatnikiem. Koszty w tym systemie mogą być ujmowane w wielu różnych przekrojach ewidencyjnych, np. według miejsc powstawania i obiektów kosztów, zarówno według wielkości rzeczywistych, jak i planowanych. Dane kosztowe zgromadzone w takim systemie mogą być wprowadzane i analizowane przez wielu różnych użytkowników. Umożliwia on korzystanie z wszelkiego rodzaju informacji zawartych w słownikach systemowych, np. klasyfikacji diagnoz ICD 10, klasyfikacji procedur medycznych ICD9, listy oddziałów i innych miejsc powstawania kosztów, list personelu medycznego. Informacje zgromadzone i przechowywane w bazie danych informatycznego systemu zarządzania szpitalem powinny umożliwiać zarządzanie kosztami w celu racjonalnego wykorzystania środków finansowych otrzymanych z Narodowego Funduszu Zdrowia w ramach zakontraktowanych świadczeń zdrowotnych.

Pojawia się jednak pytanie, jaki jest zakres stosowania i możliwości wykorzystania nowoczesnych technologii informatycznych w szpitalach i czy rzeczywiście istnieje potrzeba upowszechniania takich rozwiązań. Powszechna jest bowiem opinia, że narzędzia informatyczne, wspierające system rachunkowości zarządczej, nie są tak bardzo szpitalom potrzebne. Poza tym istnieją duże bariery psychologiczne w ich implementacji, związane m.in. z oporem pracowników medycznych. Nastawienie i zaangażowanie pracowników w proces wdrażania nowych rozwiązań organizacyjnych, zarządczych oraz proces uczenia po zakończeniu implementacji jest bowiem istotnym czynnikiem sprzyjającym wdrażaniu informatycznych systemów wspierających zarządzanie jednostką[8].

Z drugiej strony, w literaturze podkreśla się, że wykorzystanie zintegrowanych systemów informatycznych do optymalizacji podejmowanych zarządczych decyzji operacyjnych i strategicznych jest nieodzowne. Zastosowanie tych systemów umożliwia bowiem uporządkowanie wewnętrznych procesów, a także gromadzenie, przetwarzanie i selekcję danych oraz ich integrację. Wykorzystanie takich systemów w szpitalach umożliwia przede wszystkim integrowanie ze sobą danych finansowych

[8] B. Nadolna, *Bariery wdrażania informatycznego systemu controllingu w przedsiębiorstwie*, w: *Kierunki rozwoju controllingu a praktyka polskich przedsiębiorstw*, red. E. Nowak, „Prace Naukowe Akademii Ekonomicznej w Wrocławiu" 2003, nr 987.

i niefinansowych, a zwłaszcza medycznych, a zintegrowane raporty finansowe mogą być odpowiedzią na potrzeby informacyjne różnych użytkowników. Wpisywałoby się to w paradygmat strategiczno-informacyjny rachunkowości, zgodnie z którym głównym zadaniem rachunkowości jest dostarczenie informacji różnym interesariuszom[9]. Przykładowe potrzeby informacyjne różnych użytkowników informacji pochodzących ze szpitala zaprezentowano w tabeli 2.

Tabela 2. Potrzeby informacyjne użytkowników informacji finansowych szpitali

Użytkownicy	Potrzeby informacyjne
Właściciele majątku (organy założycielskie) oraz ewentualni inwestorzy	Wartość majątku, efektywność jego wykorzystania, sytuacja finansowa szpitala, zdolność do generowania przychodów, poziom wypracowanego wyniku finansowego, płynność finansowa, niezbędna do oceny stopnia ryzyka związanego z dalszym funkcjonowaniem szpitala lub zainwestowanym kapitałem i ewentualnie wysokością dywidendy (w szpitalach ukierunkowanych na zysk)
Wierzyciele (banki, pożyczkodawcy, instytucje finansowe)	Zdolność do spłaty długów wraz z odsetkami w uzgodnionych terminach, informacje o sytuacji finansowej, zasobach szpitala, zobowiązaniach, płynność finansowa oraz rentowność szpitala
Płatnicy (NFZ i inni zleceniodawcy)	Potencjał produkcyjny, gwarantujący realizację zawartych kontraktów na świadczenia zdrowotne w odpowiedniej ilości i na najwyższym poziomie jakości, koszty zrealizowanych świadczeń zdrowotnych
Pacjenci	Podaż świadczeń zdrowotnych, ich dostępność, jakość i kompleksowość, ceny świadczeń medycznych
Konkurenci (inne szpitale)	Rozmiar i kierunki działania szpitala, wielkość i struktura kosztów świadczonych usług, osiągane przychody i wyniki finansowe, słabe i mocne strony funkcjonowania szpitala
Agendy rządowe i władze terytorialne	Dane statystyczne dotyczące infrastruktury, przestrzennej lokalizacji, struktura zatrudnionych kadr medycznych, ich kwalifikacje, rozmieszczenie, wielkość zrealizowanych świadczeń medycznych i ich struktura, a także poziom zadłużenia, sytuacja finansowa, wielkość kosztów, przychodów i wyniki finansowe
Fiskus, ZUS, instytucje finansowe	Informacje dla oceny prawidłowości naliczania i rozliczania podatków (np. podatku dochodowego, podatku VAT), składek na ZUS i innych ubezpieczeń
Społeczność lokalna	Podatki lokalne, miejsca pracy, kreowanie regionalnej polityki zdrowotnej, rozwój regionu

Źródło: M. Hass-Symotiuk, D. Skrzypska, *Istota i funkcje rachunkowości ZOZ*, w: *Rachunkowość i sprawozdawczość finansowa zakładów opieki zdrowotnej*, red. M. Hass-Symotiuk, ODDK, Gdańsk 2008, s. 144–145.

Krąg odbiorców informacji dotyczących funkcjonowania szpitala i wyników jego działalności jest zatem bardzo szeroki. Wszystkie wymienione grupy interesariuszy

[9] B. Zyznarska-Dworczak, *Wiarygodność raportowania zintegrowanego w świetle strategiczno-informacyjnego paradygmatu rachunkowości*, „Studia Oeconomica Posnaniensia" 2015, 3(1), s. 191–204.

są zainteresowane sposobem, w jaki kierownictwo szpitala wykorzystuje powierzone zasoby i w tym celu potrzebują nie tylko informacji wartościowych, lecz także informacji jakościowych i ilościowych, wyrażonych w liczbach absolutnych i względnych, przedstawionych w różnych przekrojach, dotyczących szpitala i jego zamierzonej działalności, z uwzględnieniem jego otoczenia. Informacji tych ma dostarczać właśnie nowoczesny, kompleksowy i elastyczny system rachunkowości. Generowane w systemie rachunkowości informacje są zatem potrzebne do zarządzania finansami i innymi zasobami szpitali, a także do pomiaru i oceny efektywności gospodarowania, jak też do rozliczania jego kierownictwa z wytyczonych celów i zadań.

Nowe możliwości wymiany informacji pomiędzy pojedynczymi podmiotami leczniczymi a ich otoczeniem mogą pojawić się po ich włączeniu w ogólnodostępną sieć Internetu, co daje szansę usunięcia tradycyjnych barier dostępu interesariuszy zewnętrznych do danych pochodzących m.in. z systemu rachunkowości. Takie możliwości ułatwiają obecnie proces kontraktowania świadczeń medycznych i rozliczeń z płatnikiem, kształtowanie polityki cen usług medycznych i stwarzają możliwości większej przejrzystości działalności danego podmiotu oraz lepszego dostosowania zakresu udostępnianych informacji do indywidualnych potrzeb.

Dzięki wykorzystaniu systemów informatycznych użytkownicy informacji mogliby je otrzymywać z dowolną częstotliwością i w wybranym poziomie szczegółowości. Do innych korzyści płynących z wykorzystania systemów informatycznych w szpitalu można zaliczyć m.in.[10]:

- usprawnienie w prowadzeniu rachunkowości poprzez szybsze (w porównaniu z tradycyjnymi technikami) prowadzenie ewidencji księgowej, agregację i dezagregację informacji oraz sporządzanie sprawozdań finansowych,
- szybszy obieg informacji w szpitalu, możliwość otrzymywania informacji zarządczej na czas i bez opóźnień, co wpływa na szybsze podejmowanie decyzji zarządczych,
- możliwość szybkiej realizacji funkcji analitycznej rachunkowości, polegającej na badaniu i interpretacji informacji w dowolnym przekroju i o wysokim stopniu szczegółowości, pochodzących z systemu rachunkowości, oraz ocenie sytuacji finansowej i efektywności wykorzystania zasobów,
- możliwość przekazywania sprawozdań statystycznych i innych raportów w formie elektronicznej.

[10] B. Micherda, *Funkcje i struktura współczesnej rachunkowości*, w: *Podstawy rachunkowości*, red. B. Micherda, Wydawnictwo Naukowe PWN, Warszawa 2005.

Decydując się na wdrożenie takiego systemu, należy jednak pamiętać o elastyczności umożliwiającej dostosowanie poszczególnych funkcji i modułów do indywidualnych wymagań szpitala. Warto również pamiętać, aby system informatyczny szpitala był zgodny z zasadami i wymaganiami nałożonymi ustawą o rachunkowości, szczególnie w zakresie zapewnienia wiarygodności, poprawności i przejrzystości ksiąg rachunkowych oraz ochrony danych[11]. Ustawa o rachunkowości opisuje bowiem cechy ksiąg rachunkowych, prowadzonych przy wykorzystaniu komputera, obligatoryjne elementy zapisów księgowych i wydruków komputerowych, zawartość dokumentacji systemowej oraz reguluje wymagania dotyczące ochrony danych. Poza tym, aby w pełni wykorzystać możliwości takiego systemu, powinien być on prawidłowo wdrożony, co często wymaga zmiany struktury organizacyjnej samego podmiotu, wraz ze zmianą organizacji obiegu informacji i dokumentów. Proces wdrożenia takiego systemu jest długotrwały, składa się z wielu etapów, przy czym najtrudniejszym etapem jest szkolenie personelu, a najważniejszym – projektowanie potrzeb informacyjnych podmiotu[12].

4. Komputeryzacja szpitala a rachunek kosztów – przegląd literatury

W literaturze przedmiotu podkreśla się, że skuteczność narzędzi rachunkowości zarządczej, w tym rachunku kosztów, zależy od wielu różnych wewnętrznych czynników sytuacyjnych[13]. Na podstawie przeprowadzonej analizy literatury przedmiotu postawiono hipotezę badawczą, że czynnikiem, który w znacznym stopniu wpływa na jakość kalkulacji kosztów leczenia pacjenta i stopień wykorzystania informacji kosztowych w procesie zarządzania, jest stopień zinformatyzowania szpitala. Znaczenie stopnia informatyzacji szpitala w rozwoju rachunku kosztów i procesach zarządzania podkreśla się nie tylko w krajowej, lecz także w zagranicznej literaturze przedmiotu. Systemy informatyczne coraz częściej stanowią podstawę podejmowania wielu decyzji, ułatwiają dostęp do informacji potrzebnych w procesie zarządzania. Odgrywają one ogromną rolę w wewnętrznych rozliczeniach i ewidencji kosztów,

[11] Ustawa z dnia 29 września 1994 r. o rachunkowości. (t.j. Dz.U. z 2016 r., poz. 1047) – rozdział 2.

[12] K. Grabiński, *Analityczna*…, op.cit.

[13] R.H. Chenhall, *Theorising Contingencies in Management Control Systems Research*, w: *Handbook of Management Accounting Research*, red. C. Chapman, A. Hopwood, M. Shields, Elsevier, Oxford 2007, s. 165.

poprzez rozliczenia z płatnikiem aż do szeregu dodatkowych danych wykorzystywanych w procesie zarządzania[14].

Systemy informatyczne stają się coraz ważniejsze dla efektywności szpitali i dlatego muszą odpowiadać strukturze organizacyjnej tych jednostek. Stopień komputeryzacji zależy od podstawowych funkcji systemu informatycznego, przeznaczonego dla dwóch oddzielnych części struktury organizacyjnej szpitala: medycznej (białej) i administracyjnej (szarej). Na część administracyjną szpitali składają się procesy związane z obsługą kadr, finansami czy działaniem magazynów szpitalnych. Systemy informatyczne do obsługi tej części mają zatem na celu efektywne zarządzanie zasobami szpitala, kontrolę kosztów i rozliczenia z Narodowym Funduszem Zdrowia. Z kolei część medyczna dotyczy procesów związanych z obsługą wszystkich procedur medycznych, oddziałów szpitalnych, laboratoriów, pracowni diagnostycznych, sal operacyjnych i ruchu chorych w szpitalu. Warto jednak podkreślić, że stopień komputeryzacji całego szpitala zależy nie tylko od jego informatyzacji (np. wykorzystania oprogramowania, systemów komputerowych i systemów komunikacyjnych) w obszarach medycznych i administracyjnych, lecz także od integracji rozwiązań informatycznych do obsługi obu tych części na potrzeby komunikacji wewnętrznej i komunikacji z otoczeniem szpitala[15].

Wydawać by się mogło, że wysoki stopień informatyzacji medycznej i administracyjnej części szpitala oraz wysoki stopień integracji rozwiązań informatycznych w organizacji sprzyjają zastosowaniu oddolnej kalkulacji kosztów leczenia pacjenta, co poprawia jakość informacji kosztowych i sprzyja ich wykorzystaniu przez menadżerów szpitala w procesie podejmowania decyzji. Znajduje to swoje potwierdzenie w wynikach badań prezentowanych w światowej literaturze przedmiotu, które pokazują, że system rachunku kosztów wsparty technologiami informatycznymi sprzyja wykorzystaniu instrumentów rachunkowości zarządczej na potrzeby optymalizacji dokonań organizacji[16]. Systemy informatyczne pomagają poprawić przepływ informacji medycznych i finansowych, niezbędnych do przeprowadzenia czasochłonnej oddolnej kalkulacji kosztów, co podnosi jakość wyceny procesu leczenia pacjenta.

[14] J. Kaczmarska-Krawczak, *Zarządzanie informatyzacją w procesach restrukturyzacji jednostek ochrony zdrowia*, „Zarządzanie i Finanse" 2013, 1.4, s. 245–256.

[15] A. Chluski, *The Impact of Information Technology and Knowledge-Oriented Management on the Operational Effectiveness in Polish Hospitals*, „Informatyka Ekonomiczna" 2016, 39(1), s. 23–32.

[16] A.S. Maiga, A. Nilsson, F.A. Jacobs, *Assessing the Interaction Effect of Cost Control Systems and Information Technology Integration on Manufacturing Plant Financial Performance*, „The British Accounting Review" 2014, 46(1), s. 77–90.

Dzięki temu łatwiej jest pozyskać dokładne dane na potrzeby kalkulacji kosztów różnych pośrednich obiektów kosztów, takich jak procedury medyczne, osobodni leczenia, kategorie JGP, i ustalić koszty całego procesu leczenia pacjenta, nawet jeśli pacjent jest leczony w różnych oddziałach[17].

W światowej literaturze przedmiotu podkreśla się również pozytywny wpływ rozwiązań w zakresie rachunku kosztów na stopień wykorzystania informacji kosztowych w procesie zarządzania. Przeprowadzone badania pokazują bowiem, że podmioty, które w większym stopniu wykorzystują informacje kosztowe w procesie planowania i kontroli oraz przy podejmowaniu decyzji zarządczych, stosują bardziej zaawansowane systemy rachunku kosztów[18]. Z drugiej strony, inne badania wykazały, że do najważniejszych czynników, wpływających na stopień zaawansowania rachunku kosztów, należy wykorzystanie danych o kosztach w decyzjach cenowych oraz procesy związane z analizą i optymalizacją kosztów[19]. Poza tym systemy rachunku kosztów projektuje się na potrzeby ich użytkowników. Zatem jeśli menadżerowie nie wykorzystują w istotnym stopniu informacji kosztowych, zwłaszcza w procesie podejmowania decyzji, to jakość informacji kosztowych generowanych w systemie rachunku kosztów nie ma dla nich dużego znaczenia[20]. Związek między funkcjonalnością systemu rachunku kosztów, a wykorzystaniem informacji kosztowych w procesie zarządzania był również analizowany na przykładzie amerykańskich szpitali. Wyniki przeprowadzonego badania wykazały, że stopień wykorzystania informacji kosztowych w procesie zarządzania jest dodatnio skorelowany z funkcjonalnością rachunku kosztów, która wpływa na stopień szczegółowości informacji kosztowych[21].

---

[17] S.S. Tan, *Microcosting in Economic Evaluations: Issues of Accuracy, Feasibility, Consistency and Generalisability*, Erasmus Universiteit, Rotterdam 2009.

[18] O. Pavlatos, I. Paggios, *A Survey of Factors Influencing the Cost System Design in Hotels*, „International Journal of Hospitality Management" 2009, 28(2), s. 263–271.

[19] M. Al-Omiri, C. Drury, *A Survey of Factors Influencing the Choice of Product Costing Systems in UK Organizations*, „Management Accounting Research" 2007, 18(4), s. 399–424.

[20] A.I. Nicolaou, *Interactive Effects of Strategic and Cost Management Systems on Managerial Performance*, „Advances in Management Accounting" 2001, 10, s. 203–226.

[21] M.J. Pizzini, *The Relation Between Cost-System Design, Managers' Evaluations of The Relevance and Usefulness of Cost Data, and Financial Performance: An Empirical Study of US Hospitals*, „Accounting, Organizations and Society" 2006, 31(2), s. 179–210.

5. Ocena stopnia komputeryzacji szpitali, jakości kalkulacji kosztów leczenia pacjenta i wykorzystania informacji kosztowych w procesie zarządzania szpitalem

Analiza stopnia komputeryzacji szpitali została oparta na wynikach badania ankietowego przeprowadzonego w latach 2012–2013 na potrzeby oceny stanu zaawansowania rachunku kosztów i jakości wyceny świadczeń zdrowotnych w wybranych krajach europejskich. Z 221 ankiet rozesłanych do szpitali funkcjonujących w Anglii, Słowenii i Polsce, odpowiedzi udzieliły 64 jednostki, a więc około 29%. Do badań wytypowano zatem zarówno szpitale pochodzące z państwa, w którym stosowane są ujednolicone standardy rachunku kosztów (Anglia), jak i szpitale pochodzące z państw, w których takich ujednoliconych standardów brakuje (Polska, Słowenia). Wśród badanych szpitali, które odpowiedziały na ankietę, najliczniejszą grupę stanowiły szpitale polskie (30 jednostek) i angielskie (28 jednostek). Badaniami objęto szpitale podległe różnym organom założycielskim, zróżnicowane pod względem prowadzonej działalności leczniczej. Różniły się one również liczbą oddziałów i zatrudnionych pracowników, stanem infrastruktury, strukturą organizacyjną oraz wielkością środków finansowych, będących w ich dyspozycji. Warto podkreślić, że przeciętny reprezentowany w badaniu ankietowym szpital był dużym, wielooddziałowym szpitalem publicznym, znajdującym się w dużej miejscowości, zatrudniającym ponad 300 osób na stanowiskach lekarzy lub pielęgniarek[22].

Ocena stopnia komputeryzacji szpitali, dokonana przez respondentów, została przedstawiona w tabeli 3.

Tabela 3. Ocena stopnia komputeryzacji szpitala (w %)

Wyszczególnienie	Skala oceny*				
	1	2	3	4	5
Komputeryzacja części ekonomicznej			5,5	**66,5**	**28,0**
Komputeryzacja części medycznej		6,0	6,0	**82,0**	**6,0**
Zintegrowanie oprogramowania do obsługi obu części	**17,0**	**28,0**	22,0	22,0	11,0

* 1 (niedostateczna) – 5 (bardzo dobra).

Źródło: opracowanie własne.

[22] Szczegółowe informacje na temat szpitali uczestniczących w badaniu znajdują się w: M. Kludacz-Alessandri, *Model wyceny świadczeń zdrowotnych dla lecznictwa szpitalnego*, Wolters Kluwer, Warszawa 2017, s. 198.

Analiza wyników ankiety prowadzi do wniosku, że szpitale mają problem z integracją części medycznej i ekonomicznej szpitala, co może stanowić problem dostępu do danych przy wdrażaniu bardziej rozwiniętego rachunku kosztów na potrzeby doskonalenia procesu zarządzania szpitalem. Z drugiej strony wszystkie badane szpitale wykorzystują specjalistyczne oprogramowanie komputerowe dla potrzeb ekonomicznych i zdecydowana ich większość dla potrzeb medycznych. Zdecydowana większość szpitali określa stopień komputeryzacji części medycznej i ekonomicznej jako dobry lub bardzo dobry, przy czym lepiej oceniana jest komputeryzacja części ekonomicznej.

Jakość rachunku kosztów w szpitalach i stopień wykorzystania informacji kosztowych w procesie zarządzania zmierzono, wykorzystując pięciostopniową skalę Likerta[23]. Pytania zawarte w ankiecie miały m.in. na celu określenie stopnia dokładności kalkulacji kosztów leczenia pacjenta. Odpowiedzi respondentów dotyczące poszczególnych etapów kalkulacji kosztów leczenia pacjenta przedstawiono w tabeli 4.

Tabela 4. Etapy wyceny procesu leczenia pacjenta (w %)

Etapy wyceny	Skala oceny*				
	1	2	3	4	5
Pomiar materiałów bezpośrednich zużywanych przez pacjenta	10,0	10,0	17,0	25,0	38,0
Pomiar kosztów robocizny bezpośredniej wykonanej na rzecz pacjenta	12,5	16,0	5,0	31,5	35,0
Doliczanie kosztów procedur medycznych wykonanych na rzecz pacjenta	9,5	13,0	8,0	22,5	47,0
Doliczanie kosztów osobodni opieki pobytu pacjenta na oddziale	12,5	10,0	12,5	16,0	49,0
Alokowanie innych kosztów pośrednich na rzecz pacjenta, np. kosztów zarządu	19,0	9,5	9,5	13,0	49,0

* 1 (zdecydowanie nie dotyczy) – 5 (zdecydowanie dotyczy).

Źródło: opracowanie własne.

Większość badanych szpitali stara się stosować oddolną kalkulację netto i przyporządkowuje część kosztów bezpośrednio do procesu leczenia pacjenta, a także dokonuje wcześniejszej wyceny pośrednich obiektów kosztów, kalkulując koszty procedur medycznych wykonanych na rzecz pacjenta oraz koszty osobodni pobytu

[23] Skala Likerta to pięciostopniowa skala, wykorzystywana w kwestionariuszach ankiet i wywiadach kwestionariuszowych, dzięki której uzyskać można odpowiedź, dotyczącą stopnia akceptacji zjawiska, poglądu itp. Bardzo często jest stosowana do mierzenia postaw wobec konkretnych problemów czy opinii. Więcej na ten temat w: R. Likert, *A Technique for the Measurement of Attitudes*, „Archives of Psychology" 1932, 140, 55.

pacjenta na oddziale. Jednak około 10% szpitali nie alokuje kosztów bezpośrednich do procesu leczenia pacjenta i nie kalkuluje kosztów obiektów częściowych, ograniczając się jedynie do odgórnej kalkulacji brutto.

W literaturze przedmiotu podkreśla się, że podstawową funkcją systemu rachunku kosztów jest wspieranie decyzji menedżerskich i procesu kontroli[24]. W przeprowadzonych analizach zbadano zatem stopień wykorzystania różnych instrumentów rachunkowości zarządczej w szpitalach. W tym celu poproszono respondentów o ocenę stopnia wykorzystania informacji kosztowych w różnych aspektach związanych z zarządzaniem szpitalem, np.: negocjacje cenowe z płatnikiem, analizy Jednorodnych Grup Pacjentów (porównywanie kosztów z cenami w przekroju JGP), analizy rentowności, decyzje cenowe (wyznaczanie cen usług medycznych), ocena dokonań, ustalanie struktury asortymentowej usług (zaniechanie świadczenia określonych usług, oferowanie nowych usług). Otrzymane wyniki zaprezentowano w tabeli 5.

Tabela 5. Ocena stopnia wykorzystania informacji kosztowych w wybranych procesach zarządzania szpitalem

Wyszczególnienie	Skala oceny* (w %)					MV
	1	2	3	4	5	
Budżetowanie i planowanie	–	11,1	11,1	16,7	61,1	4,28
Kontrola kosztów	–	–	11,1	22,2	66,7	4,56
Negocjacje kontraktów z płatnikiem	5,6	27,8	11,1	11,1	44,4	3,61
Analizy JGP	27,8	11,1	27,8	11,1	22,2	2,89
Analizy rentowności	–	16,7	22,2	27,8	33,3	3,78
Decyzje cenowe	–	11,1	16,7	38,9	33,3	3,94
Usprawnianie procesów	11,1	11,1	16,7	27,8	33,3	3,61
Ocena dokonań	16,7	–	22,2	22,2	38,9	3,67
Ustalanie, zmiana standardów medycznych	33,3	–	27,8	22,2	16,7	2,89
Decyzje w sprawie nabycia sprzętu medycznego	11,1	–	22,3	33,3	33,3	3,78
Raportowanie zewnętrzne	16,7	5,6	22,2	22,2	33,3	3,50
Benchmarking – porównania z innymi szpitalami	22,2	38,9	11,1	–	27,8	2,72
Ocena efektywności wykorzystania zasobów	11,1	5,6	22,2	33,3	27,8	3,61

* 1 (w niedostatecznym stopniu) – 5 (w bardzo dużym stopniu), MV – średnia,

Źródło: opracowanie własne.

[24] M.A. Abernethy, J. Bouwens, *Determinants of Accounting Innovation Implementation*, „Abacus" 2005, 41, s. 217–239.

Z przedstawionych danych wynika, że informacje kosztowe są wykorzystywane we wszystkich procesach zarządzania, jednak tylko w nielicznych przypadkach na poziomie znacznie przekraczającym średnią. Menedżerowie szpitali wykorzystują informacje kosztowe przede wszystkim na wewnętrzne potrzeby szpitala, zwłaszcza w procesie budżetowania i kontroli kosztów, a także do: analizy rentowności, wyznaczania cen usług medycznych i podejmowania decyzji w sprawie nabycia sprzętu medycznego, oceny dokonań oraz oceny efektywności wykorzystania zasobów. Najmniej istotną rolę informacje te odgrywają w procesach zewnętrznych, takich jak: benchmarking czy raportowanie zewnętrzne.

6. Ocena wpływu stopnia komputeryzacji szpitala na jakość kalkulacji leczenia pacjenta i stopień wykorzystania informacji kosztowych w procesie zarządzania szpitalem

Zgodnie z postawioną w części teoretycznej hipotezą założono, że wyższy stopień komputeryzacji szpitala wpływa na lepszą jakość kalkulacji kosztów leczenia pacjenta i prowadzi do bardziej efektywnego wykorzystania informacji w procesach zarządzania, opartych na analizach kosztowo-cenowych. W celu weryfikacji tej hipotezy zastosowano analizę regresji wielorakiej, która pozwala na ocenę siły i formy związku między zmiennymi, a także na predykcję jednej zmiennej na podstawie zaobserwowanych skorelowanych z nią wartości innych zmiennych[25]. W celu pomiaru zależności pomiędzy badanymi zmiennymi wykorzystano metodę częściowej agregacji poszczególnych zmiennych reprezentujących wielowymiarowe konstrukty[26]. Przykładowo, dla zmiennej „jakość komputeryzacji" obliczono średnią z trzech wskaźników, takich jak: stopień komputeryzacji części ekonomicznej szpitala, stopień komputeryzacji części medycznej szpitala i stopień zintegrowania oprogramowania do obsługi części medycznej i ekonomicznej.

Szczególną uwagę zwrócono na możliwość wielowymiarowości dwóch zmiennych: jakości kalkulacji kosztów leczenia pacjenta i wykorzystania informacji kosztowych w procesie zarządzania. W celu przygotowania ostatecznych elementów

[25] R. Konarski, *Modele równań strukturalnych*, Wydawnictwo Naukowe PWN, Warszawa 2009.

[26] R.P. Bagozzi, J.R. Edwards, *A General Approach for Representing Constructs in Organizational Research*, „Organizational Research Methods" 1998, 1, s. 45–187.

wymienionych konstuktów przeprowadzono analizę czynnikową. Jej celem jest wyodrębnienie wszystkich czynników, które mogą rzeczywiście tkwić w korelacjach danego układu zmiennych, jednocześnie zachowując jak najwięcej informacji zawartych w zmiennych pierwotnych, a następnie redukcja tych czynników[27]. Analizie czynnikowej poddano wszystkie pozycje ankiety, dotyczące poszczególnych etapów kalkulacji kosztów leczenia pacjenta i poszczególnych narzędzi rachunkowości zarządczej, wykorzystywane przez dyrektorów szpitali. Ostatecznie, po przeprowadzeniu analizy czynnikowej, do pomiaru konstruktu „jakość kalkulacji kosztów leczenia pacjenta" weszły cztery wskaźniki, a do pomiaru konstruktu „wykorzystanie informacji kosztowych w procesie zarządzania" dwa wskaźniki.

Przed przeprowadzeniem analizy regresji przeprowadzono analizę korelacji. Współczynniki korelacji pomiędzy zmiennymi analizowanego modelu przedstawiono w tabeli 6.

Tabela 6. Współczynniki korelacji pomiędzy analizowanymi zmiennymi

Analizowane zmienne	SI	JKP	WIK
Stopień informatyzacji, SI	1		
Jakość kalkulacji procesu leczenia pacjenta, JKP	**0,43****	1	
Wykorzystanie informacji kosztowych w zarządzaniu, WIK	0,08	**0,42****	1

* Współczynnik istotny statystycznie na poziomie $p < 0{,}01$.
** Współczynnik istotny statystycznie na poziomie $p < 0{,}05$.

Źródło: opracowanie własne.

Na trzy związki przedstawione w tabeli, dwa są istotne statystycznie ($p < 0{,}05$), w tym jeden, który ma istotne znaczenie w tej analizie, biorąc pod uwagę cel badania (został on przedstawiony w zaznaczonej na szaro komórce tabeli), gdyż jest on spójny z postawioną hipotezą badawczą. Nie wykazano natomiast istotnego związku między stopniem informatyzacji szpitala a wykorzystaniem informacji kosztowych w zarządzaniu. Związki pomiędzy badanymi zmiennymi potwierdziła analiza regresji wielorakiej, w której przeanalizowano wpływ różnych zmiennych strukturalnych na jakość kalkulacji kosztów leczenia pacjenta i wykorzystanie informacji kosztowych w procesie zarządzania.

[27] A. Czopek, *Analiza porównawcza efektywności metod redukcji zmiennych – analiza składowych głównych i analiza czynnikowa*, „Studia Ekonomiczne" 2013, 132, s. 7–23.

Wśród zmiennych niezależnych uwzględniono, oprócz jakości komputeryzacji, również wykształcenie dyrektora szpitala i wielkość szpitala. Ostateczny dobór zmiennych przeprowadzono metodą regresji krokowej „wstecz"[28]. Standaryzowane współczynniki regresji (beta), reprezentujące wpływ poszczególnych predyktorów na zmienne wyjaśniane reprezentowane przez dwa czynniki, zostały przedstawione w tabeli 7.

Tabela 7. Wyniki analizy regresji wielorakiej

Analizowane zmienne	Czynnik I JKP	Czynnik II WIK
Wykształcenie menedżerów, WM	–	–0,39**
Wielkość szpitala, WS	0,39*	–
Stopień informatyzacji, SI	0,39*	–
Jakość kalkulacji procesu leczenia pacjenta, JKP	–	0,42**
Wykorzystanie informacji kosztowych w zarządzaniu, WIK	–	–
Współczynnik dyskryminacji, R^2	0,33	0,33
Statystyka F	5,3***	8,17**

* Współczynnik istotny statystycznie na poziomie $p < 0,05$.
** Współczynnik istotny statystycznie na poziomie $p < 0,01$.
Źródło: opracowanie własne.

Wyniki przeprowadzonej analizy wykazały, że zmienne objaśniające dobrze wyjaśniały zmienność zmiennej zależnej, a wskazane zależności były poprawne merytorycznie. Predyktory uwzględnione w analizie wyjaśniają w przybliżeniu 33% zmienności czynnika pierwszego (jakość kalkulacji kosztów leczenia pacjenta) i czynnika drugiego (wykorzystanie informacji kosztowych w procesie zarządzania). Wyniki analizy regresji potwierdziły, że istnieją statystycznie istotne związki pomiędzy stopniem informatyzacji szpitala a jakością kalkulacji kosztów leczenia pacjenta. Potwierdziło się też, że nie ma żadnych istotnych statystycznie związków pomiędzy stopniem jego informatyzacji a wykorzystaniem informacji kosztowych w procesie zarządzania. Może to wynikać z tego, że dyrektorzy analizują informacje kosztowe już we własnym zakresie, nie korzystając przy tym z systemu komputerowego. Z drugiej strony, analiza korelacji wykazała związek pomiędzy jakością

[28] D. Witkowska, *Metody statystyczne w zarządzaniu*, Wydawnictwo Wydziału Organizacji i Zarządzania Politechniki Łódzkiej, Łódź 1999, s. 240–241.

kalkulacji kosztów leczenia pacjenta a stopniem wykorzystania informacji kosztowych w procesie zarządzania. Lepsza jakość kalkulacji kosztów leczenia pacjenta wpływa zatem na lepsze wykorzystanie informacji kosztowych przez dyrektorów szpitala.

7. Podsumowanie

W literaturze przedmiotu podkreśla się, że powszechne wykorzystanie technologii informatycznych jest niewątpliwie najistotniejszą tendencją z perspektywy systemu informacyjnego rachunkowości, niezbędnego do efektywnego funkcjonowania podmiotów i całych systemów gospodarczych[29]. Systemy informatyczne wspierające system rachunkowości na stałe zagościły również w podmiotach leczniczych, na co wpłynęło systematyczne zwiększenie parametrów technicznych sprzętu komputerowego, rozpowszechnienie zestandaryzowanego oprogramowania, m.in. do rozliczania kontraktów z Narodowym Funduszem Zdrowia.

Przeprowadzone badania pokazały, że czynnikiem strukturalnym, który ma największe znaczenie dla jakości wyceny procesu leczenia pacjenta, okazała się jakość informatyzacji szpitala. Co wynika z tego, że wysoki poziom komputeryzacji części medycznej i ekonomicznej umożliwia ewidencję różnych kategorii kosztów w różnych przekrojach, np. rodzajowym, według miejsc powstawania i w przekroju przedmiotowym, tj. poszczególnych pacjentów i kategorii JGP, nawet w sytuacji, gdy pacjent leczony jest na różnych oddziałach. Wysoki stopień zintegrowania oprogramowania do obsługi części medycznej i ekonomicznej ułatwia stosowanie oddolnej kalkulacji kosztów netto, co podnosi jakość kalkulacji kosztów i pomaga w usprawnieniu przepływu informacji medycznych i finansowych, których powiązanie jest konieczne przy ustalaniu kosztów poniesionych na realizowane świadczenia zdrowotne. Dzięki temu można uzyskać dokładne dane dotyczące kosztów jednostkowych wszystkich procedur wykonywanych w szpitalu i ich przypisanie do poszczególnych pacjentów. Z przeprowadzonej analizy wynika również, że lepsza jakość kalkulacji procesu leczenia pacjenta wpływa pozytywnie na stopień wykorzystania informacji kosztowych w zarządzaniu szpitalem. Lepsze informacje generowane z systemu rachunku kosztów ułatwiają bowiem prowadzenie analiz kosztowych przez kierownictwo szpitala, a tym samym wpływają na lepsze decyzje menedżerskie oparte na tych analizach.

[29] M. Łada, *Rachunkowość i nowe technologie*, w: *Rachunkowość w otoczeniu nowych technologii*, red. M. Łada, A. Kozarkiewicz, C.H. Beck, Warszawa 2008.

Bibliografia

Dokumenty prawne

1. Ustawa z dnia 29 września 1994 r. o rachunkowości. (t.j. Dz.U. z 2016 r., poz. 1047).

Wydawnictwa zwarte

1. Abernethy M.A., Bouwens J., *Determinants of Accounting Innovation Implementation*, „Abacus" 2005, 41.
2. Al-Omiri M., Drury C., *A Survey of Factors Influencing the Choice of Product Costing Systems in UK Organizations*, „Management Accounting Research" 2007, 18(4).
3. Bagozzi R.P., Edwards J.R., *A General Approach for Representing Constructs in Organizational Research*, „Organizational Research Methods" 1998, 1.
4. Brzezin W., *Ogólna teoria rachunkowości*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 1995.
5. Burzym E., *Rachunkowość przedsiębiorstw i instytucji*, PWE, Warszawa 1980.
6. Chenhall R.H., *Theorising Contingencies in Management Control Systems Research*, w: *Handbook of Management Accounting Research*, red. C. Chapman, A. Hopwood, M. Shields, Elsevier, Oxford 2007.
7. Chluski A., *The Impact of Information Technology and Knowledge-Oriented Management on The Operational Effectiveness in Polish Hospitals*, „Informatyka Ekonomiczna" 2016, 39(1).
8. Czopek A., *Analiza porównawcza efektywności metod redukcji zmiennych – analiza składowych głównych i analiza czynnikowa*, „Studia Ekonomiczne" 2013, 132.
9. Grabiński K., *Analityczna funkcja rachunkowości w systemach informatycznych klasy ERP*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2005, nr 674.
10. Hass-Symotiuk M., *Rachunkowość jako system generowania informacji ekonomiczno-finansowych na potrzeby zarządzania w zakładzie opieki zdrowotnej*, w: *Rachunkowość. System informacji finansowych Zakładów Opieki Zdrowotnej*, red. M. Hass-Symotiuk, Wolters Kluwer Polska, Warszawa 2010.
11. Hass-Symotiuk M., Skrzypska D., *Istota i funkcje rachunkowości ZOZ*, w: *Rachunkowość i sprawozdawczość finansowa zakładów opieki zdrowotnej*, red. M. Hass-Symotiuk, ODDK, Gdańsk 2008.
12. Jaruga A., Sobańska I., Kopczyńska L. i in., *Rachunkowość dla menedżerów*, wyd. II, Towarzystwo Gospodarcze RAFIB, Łódź 1994.
13. Kaczmarska-Krawczak J., *Zarządzanie informatyzacją w procesach restrukturyzacji jednostek ochrony zdrowia*, „Zarządzanie i Finanse" 2013, 1.4.

14. Kludacz M., *Rachunek kosztów i jego wykorzystanie w zarządzaniu szpitalem*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu 2015, vol. 389.
15. Kludacz-Alessandri M., *Model wyceny świadczeń zdrowotnych dla lecznictwa szpitalnego*, Wolters Kluwer, Warszawa 2017.
16. Konarski R., *Modele równań strukturalnych*, Wydawnictwo Naukowe PWN, Warszawa 2009.
17. Król-Stępień M., *System informatyczny rachunkowości jako narzędzie wspomagające zarządzanie jednostką gospodarczą – wymogi ustawowe, a ich praktyczne zastosowanie*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2013, nr 757, „Finanse, Rynki Finansowe, Ubezpieczenia" nr 58.
18. Kunz B., Tymińska A., *System informatyczny rachunkowości i jego rola w świetle ustawy o rachunkowości*, „Nauki o Finansach" 2014, 3.
19. Likert R., *A Technique for the Measurement of Attitudes*, „Archives of Psychology" 1932, 140, 55.
20. Łada M., *Rachunkowość i nowe technologie*, w: *Rachunkowość w otoczeniu nowych technologii*, red. M. Łada, A. Kozarkiewicz, C.H. Beck, Warszawa 2008.
21. Maiga A.S., Nilsson A., Jacobs F.A., *Assessing the Interaction Effect of Cost Control Systems and Information Technology Integration on Manufacturing Plant Financial Performance*, „The British Accounting Review" 2014, 46(1).
22. Micherda B., *Analityczna funkcja rachunkowości*, Wydawnictwo AE w Krakowie, Kraków 2001.
23. Micherda B., *Funkcje i struktura współczesnej rachunkowości*, w: *Podstawy rachunkowości*, red. B. Micherda, Wydawnictwo Naukowe PWN, Warszawa 2005.
24. Nadolna B., *Bariery wdrażania informatycznego systemu controllingu w przedsiębiorstwie*, w: *Kierunki rozwoju controllingu a praktyka polskich przedsiębiorstw*, red. E. Nowak, „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 2003, nr 987.
25. Nicolaou A.I., *Interactive Effects of Strategic and Cost Management Systems on Managerial Performance*, „Advances in Management Accounting" 2001, 10.
26. Niziński S., Żurek J., Liger K., *Logistyka dla inżynierów*, Wydawnictwo Komunikacji i Łączności, Warszawa 2011.
27. Pavlatos O., Paggios I., *A Survey of Factors Influencing the Cost System Design in Hotels*, „International Journal of Hospitality Management" 2009, 28(2).
28. Pizzini M.J., *The Relation Between Cost-System Design, Managers' Evaluations of The Relevance and Usefulness of Cost Data, and Financial Performance: An Empirical Study of US Hospitals*, „Accounting, Organizations and Society" 2006, 31(2).
29. *Rachunkowość finansowa*, red. K. Sawicki, PWE, Warszawa 1999.

30. Sadowska B., *Znaczenie i warunki stosowania zintegrowanych systemów informatycznych w sferze budżetowej*, „Zeszyty Teoretyczne Rachunkowości" 2014, t. 76(132).
31. Tan S.S., *Microcosting in Economic Evaluations: Issues of Accuracy, Feasibility, Consistency and Generalisability*, Erasmus Universiteit, Rotterdam 2009.
32. Turyna J., *System informacyjny rachunkowości*, Wydawnictwa Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa 1997.
33. Zyznarska-Dworczak B., *Wiarygodność raportowania zintegrowanego w świetle strategiczno-informacyjnego paradygmatu rachunkowości*, „Studia Oeconomica Posnaniensia" 2015, 3(1).

The Impact of the Level Hospital Computerisation on the Healthcare Service Cost Calculation

Summary

An effective evaluation of the patient treatment process requires detailed cost information from the health care entity accounting system. The most important tool to support the accounting system, and in particular the process of calculation of health care services, is an IT system designed in such a way as to allow for the integration of the financial and medical hospital data.

The article is aimed at the analysis of the hospital computerisation level and the assessment of the impact of this factor on the quality of solutions with regard to the cost calculation of the patient treatment process and the level of use of cost information in the process of hospital management. This evaluation was made on the basis of results of empirical research conducted in Polish, English, and Slovenian hospitals. On the basis of the literature analysis a research hypothesis was posed that the factor which strongly affects the quality of the patient treatment cost calculation and the level of use of cost information in the hospital management process is the level of hospital informatisation. The verification of the research hypothesis was based on the correlation analysis and multiple regression. The research indicates that the level of hospital computerisation is a factor which most affects the quality of calculation patient treatment costs, which in turn affects the level of use of cost information in the hospital management process.

Keywords: IT system, cost account, patient treatment cost calculation

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 129–143

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

Beata Sadowska
Katedra Rachunkowości i Controllingu
Uniwersytet Szczeciński, WZiEU

System Informatyczny Lasów Państwowych – nowoczesne narzędzie informatyczne wykorzystywane w systemie rachunkowości

Streszczenie

Sprawne funkcjonowanie współczesnych organizacji uzależnione jest od stopnia zorganizowania oraz zinformatyzowania działań i procesów gospodarczych. Zintegrowany system informatyczny jednostki gospodarczej składa się z wielu współpracujących ze sobą systemów, które mają za zadanie ujmowanie pełnego zakresu zdarzeń i operacji gospodarczych oraz dostarczanie wielu rzetelnych, aktualnych informacji na potrzeby użytkowników wewnętrznych i zewnętrznych. Celem głównym opracowania będzie odpowiedź na pytanie badawcze: Czy System Informatyczny Lasów Państwowych (SILP[1]) pozwala na generowanie i prezentowanie kompleksowej informacji o działalności Lasów Państwowych? Celem szczegółowym będzie odpowiedź na pytanie: Czy stopień złożoności systemu SILP generuje szumy informatyczne? Zastosowano następujące metody badawcze: studia literaturowe, analizę, wnioskowanie. Niezbędna była również dogłębna analiza źródeł prawa zewnętrznego oraz wewnętrznego Lasów Państwowych.

[1] W opracowaniu autorka będzie się posługiwała skrótem SILP mając na myśli System Informatyczny Lasów Państwowych.

Słowa kluczowe: Lasy Państwowe, system informatyczny, podsystem finansowo-księgowy, rachunkowość
Kody klasyfikacji JEL: M41, Q23, Q56, C88

1. Wprowadzenie

Każda jednostka gospodarcza potrzebuje wdrażania lub ciągłej optymalizacji rozwiązań informatycznych wspierających jej działania. Współcześnie trudno jest efektywnie świadczyć usługi, oferować produkty czy realizować zadania bez spójnej i wiarygodnej bazy danych, która dostarcza bieżącej informacji o działalności organizacji. Szczególną rolę odgrywają zintegrowane systemy informatyczne ze szczególnym uwzględnieniem podsystemów finansowo-księgowych.

Niniejsze opracowanie ma charakter opisowy i wyjaśniający. Dotyczy prezentacji zintegrowanego oprogramowania Państwowego Gospodarstwa Leśnego Lasy Państwowe (PGL LP[2]) jako elementu architektury rozproszonego przetwarzania danych. Celem głównym będzie odpowiedź na pytanie badawcze: Czy System Informatyczny Lasów Państwowych (SILP) pozwala na generowanie i prezentowanie kompleksowej informacji o działalności Lasów Państwowych? Celem szczegółowym będzie odpowiedź na pytanie: Czy stopień złożoności systemu SILP generuje szumy informatyczne?

Zastosowano następujące metody badawcze: studia literaturowe, analizę, wnioskowanie. Niezbędna była również dogłębna analiza źródeł prawa zewnętrznego oraz wewnętrznego Lasów Państwowych.

2. System informatyczny w rachunkowości – przegląd literatury przedmiotu

W XX w. informacja stała się jednym z kluczowych zasobów każdej organizacji. Informacja oraz jej przekaz nabierają coraz większego znaczenia[3]. Brak rzetelnych

[2] W opracowaniu autorka będzie się posługiwała skrótem PGL LP lub LP, mając na myśli Państwowe Gospodarstwo Leśne Lasy Państwowe.

[3] R. Angryk, *E-gospodarka*, w: *Inżynieria systemów informatycznych w e-gospodarce*, red. E. Kolbusz, W. Olejniczak, Z. Szyjewski, PWE, Warszawa 2005, s. 15.

informacji powoduje, że decyzje gospodarcze mogą być podejmowane na podstawie przypuszczeń, domysłów, szacunków, dotychczasowych doświadczeń, danych historycznych lub fragmentarycznych. Ustawa z dnia 29 września 1994 r. o rachunkowości[4] nakłada na wszystkie podmioty i jednostki prowadzące księgi rachunkowe obowiązek posiadania aktualnej dokumentacji, określającej przyjęte w jednostce zasady, zwane polityką rachunkowości, której integralną częścią jest opis stosowanego systemu informatycznego[5], w celu generowania użytecznych informacji.

Zgodzić się należy z **A. Lulkiem**, że system informacyjny przedsiębiorstwa tworzony jest między innymi przez system informacyjny rachunkowości[6]. Stosowanie systemów informatycznych w podmiocie gospodarczym umożliwia sprawne i skuteczne realizowanie różnych funkcji rachunkowości, jak wskazuje **B. Micherda**[7]. Ponadto **B. Nadolna** podkreśla, że system informatyczny powinien mieć następujące cechy: wiarygodność, sprawdzalność oraz dogodność i elastyczność w eksploatacji[8]. Systemy informatyczne to narzędzia udostępniające użytkownikom obszerną funkcjonalność, która umożliwia przetwarzanie dużej ilości danych. **M. Łada**[9] zwraca uwagę, że: „współczesna rachunkowość przechodzi gwałtowną transformację, która jest konsekwencją powszechnego wykorzystania technologii informatycznych".

Praktyka gospodarcza potwierdza, iż znaczącą rolę odgrywa obecnie zintegrowany system informatyczny przedsiębiorstwa, który składa się z wielu podsystemów współpracujących ze sobą. Szerzej procesy te opisuje **A. Bytniewski**[10], podkreślając,

---

[4] Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2013 r. poz. 330 z późn. zm.)

[5] B. Sadowska, *Znaczenie i warunki stosowania zintegrowanych systemów informatycznych w sferze budżetowej*, „Zeszyty Teoretyczne Rachunkowości" 2014, nr 76(132), s. 62.

[6] A. Lulek, *Od przeszłości do przyszłości – ewolucja rachunkowości i jej pojęcia*, w: *Dylematy i perspektywy rozwoju finansów i rachunkowości*, red. P. Szczypa, A. Zimny, Wydawnictwo Państwowej Wyższej Szkoły Zawodowej w Koninie, Konin 2017, s. 95.

[7] Autor wskazuje na funkcje: informacyjną, kontrolną, analityczną, stymulacyjną (zarządczą), statystyczną; B. Micherda, *Funkcje i struktura współczesnej rachunkowości*, w: *Podstawy rachunkowości*, red. B. Micherda, Wydawnictwo Naukowe PWN, Warszawa 2005, s. 14.

[8] Szerzej: B. Nadolna, *Dostosowanie informatycznych systemów rachunkowości do potrzeb zarządzania*, „Zeszyty Teoretyczne Rady Naukowej Stowarzyszenia Księgowych w Polsce" 2006, nr 35.

[9] M. Łada, *Automatyzacja procesów rachunkowości zarządczej*, w: *Rachunkowość a controlling*, red. E. Nowak, M. Kowalewski, M. Nieplowicz, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2016, nr 440, s. 393.

[10] A. Bytniewski, *Podsystem controlingu w ramach zintegrowanego systemu zarządzania jako źródło informacji na potrzeby rachunkowości zarządczej i controllingu*, w: *Rachunkowość a controlling*, red. E. Nowak, M. Kowalewski, M. Nieplowicz, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2016, nr 440, s. 73.

że sprawne funkcjonowanie współczesnych przedsiębiorstw uzależnione jest od stopnia zorganizowania i zinformatyzowania ewidencji procesów gospodarczych.

Zintegrowany system informatyczny jest systemem informacyjnym, w którym do rozwiązywania problemów zarządzania wykorzystuje się technikę komputerową. Powinien być ukierunkowany na zaspokajanie potrzeb menedżerów. Zintegrowany system informatyczny nie jest tylko oprogramowaniem, to cała filozofia pracy organizacji, to komunikacja, koordynacja, wiedza i informacja, to praca ludzi.

Podsystem finansowo-księgowy ujmuje pełen zakres zdarzeń gospodarczych w organizacji, pozwala w sposób automatyczny przenosić dane z innych podsystemów, automatycznie je dekretować i księgować. Charakteryzuje się wysoką sprawnością dostarczania danych w krótkich okresach, co skutkuje wyższą efektywnością realizowanych zadań, wyższą jakością oferowanych produktów i usług oraz racjonalną gospodarką w zakresie prowadzonej działalności operacyjnej.

3. Specyfika i model funkcjonowania Państwowego Gospodarstwa Leśnego Lasy Państwowe

PGL LP jest jednostką organizacyjną nieposiadającą osobowości prawnej, niebędącą przedsiębiorstwem w rozumieniu prawa, działającą na terenie Polski. Nie należy do sektora przedsiębiorstw ani do sektora finansów publicznych. Podstawowym dokumentem określającym działalność PGL LP jest ustawa o lasach[11] z 28 września 1991 r. Określa ona zasady prowadzenia gospodarki leśnej zarówno przez LP, jak i w lasach innych własności. Strukturę organizacji precyzuje jej statut[12], wydany zarządzeniem ministra środowiska z 1994 r. oraz Strategia PGL LP na lata 2014–2030[13].

Zgodnie z ustawą o lasach w skład PGL LP wchodzą następujące jednostki organizacyjne:

- Dyrekcja Generalna LP,
- regionalne dyrekcje LP,
- nadleśnictwa,
- jednostki organizacyjne, zwane dalej „zakładami".

[11] Ustawa z dnia 28 września 1991 r. o lasach (Dz.U. z 1991 r. nr 101, poz. 444 z późn. zm.)

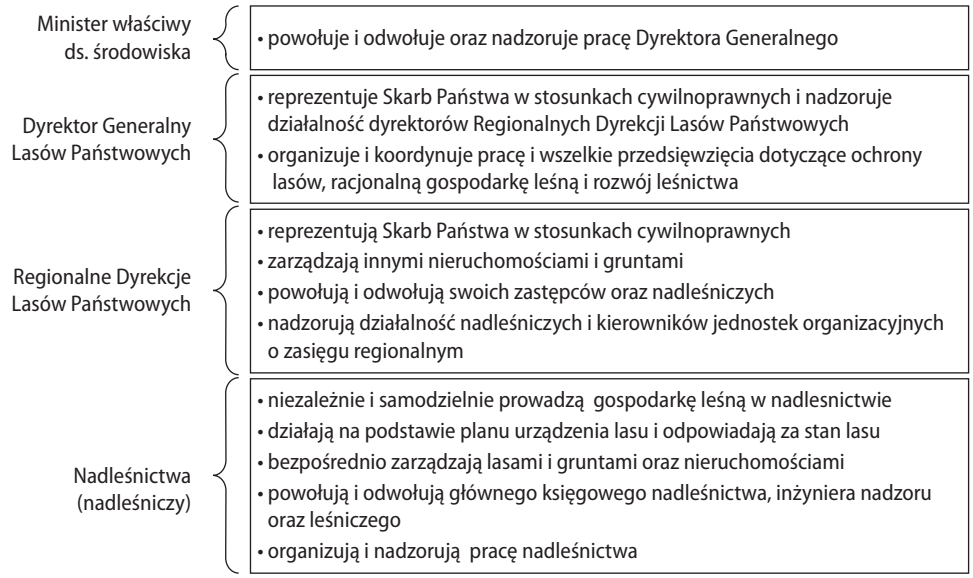
[12] Statut PGL LP, http://bip.lasy.gov.pl

[13] Strategia PGL LP na lata 2014–2030, http://bip.lasy.gov.pl

Na potrzeby niniejszego opracowania badaniu poddano wybrane nadleśnictwa w Polsce. Na podstawie rozmów prowadzonych z pracownikami nadleśnictw zbierano informacje na temat funkcjonowania systemów informatycznego i informacyjnego, wykorzystywanego przez te jednostki[14]. Badanie prowadzono w okresie październik–listopad 2016 r.

Elementem rachunku ekonomicznego i podstawą gospodarki finansowej jednostek organizacyjnych LP są sporządzane przez nie roczne plany finansowo-gospodarcze, zawierające[15]: zadania rzeczowe, przychody ze sprzedaży, koszty działalności, wynik finansowy. Organizacja i podstawowe zadania LP zostały zaprezentowane na rysunku 1.

Rysunek 1. Organizacja i podstawowe zadania Lasów Państwowych



Źródło: opracowanie własne na podstawie Ustawy z dnia 28 września 1991 r. o lasach.

[14] Należy podkreślić, że SILP jest systemem zintegrowanym. Praca w systemie może być prowadzona w różnych modułach przez odpowiednio uprawnionych pracowników nadleśnictw, leśnictw, oddziałów Regionalnych Dyrekcji. Informacje mogą być generowane i dostępne z każdego poziomu jednostki organizacyjnej PGL LP. W Polsce jest 430 nadleśnictw, które pracują na podstawie tego samego systemu informatycznego, jedynego takiego programu, dedykowanego właśnie dla PGL LP.

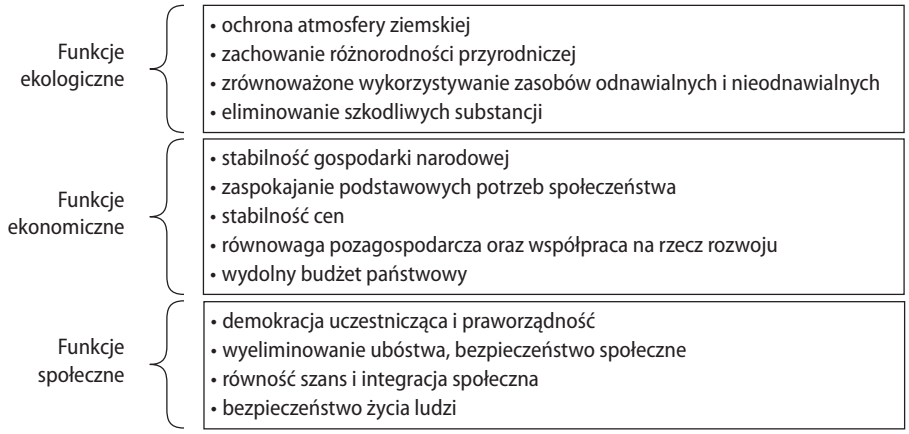
[15] Rozporządzenie Rady Ministrów z dnia 6 grudnia 1994 r. w sprawie szczegółowych zasad gospodarki finansowej w Państwowym Gospodarstwie Leśnym Lasy Państwowe (Dz.U. z 1994 r. nr 134, poz. 692).

Zgodnie z postanowieniami Ustawy z dnia 28 wrzenia 1991 r. o lasach[16], głównym celem PGL LP jest prowadzenie gospodarki leśnej według zasad:

- powszechnej ochrony lasów oraz trwałości ich utrzymania,
- ciągłości i zrównoważonego wykorzystania wszystkich funkcji lasów,
- powiększania zasobów leśnych.

Cele PGL LP są realizowane przez funkcje przedstawione na rysunku 2.

Rysunek 2. Funkcje PGL LP



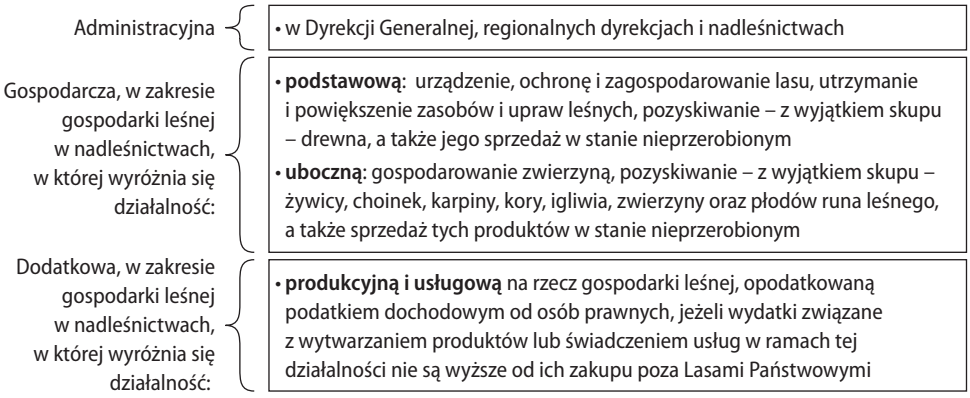
Źródło: opracowanie własne na podstawie: H. Roggal, *Ekonomia zrównoważonego rozwoju*, Wydawnictwo Zysk i S-ka, Poznań 2010, s. 47.

Zgodnie z postanowieniem ustawy o lasach, rozporządzeniami i zarządzeniami wydanymi na podstawie tej ustawy, głównym celem PGL LP jest prowadzenie gospodarki leśnej według podstawowych zasad, do których można zaliczyć: powszechną ochronę lasów, trwałość ich utrzymania, zrównoważone wykorzystanie poszczególnych funkcji lasów oraz powiększanie zasobów leśnych. Cel ten jest realizowany przez trwale zrównoważoną, wielofunkcyjną gospodarkę leśną, która jest prowadzona zgodnie z planem urządzenia lasu opracowywanym dla każdego nadleśnictwa na okres dziesięcioletni. W LP i ich jednostkach organizacyjnych, w ramach sprawowanego zarządu, działalność jest prowadzona na podstawie rachunku ekonomicznego[17]. Poszczególne elementy tej działalności zaprezentowano na rysunku 3.

[16] Ustawa z dnia 28 września 1991 r. o lasach.

[17] Zob.: B. Sadowska, *Strategia Państwowego Gospodarstwa Leśnego Lasy Państwowe a zrównoważony rozwój*, w: *Finanse na rzecz zrównoważonego rozwoju. Gospodarka – etyka – środowisko*,

Rysunek 3. Elementy działalności Lasów Państwowych



Źródło: jak pod rys. 1.

Działalność gospodarczo-leśna jest prowadzona na podstawie zasad ochrony i trwałości lasów, jednakże należy zwrócić uwagę na fakt, że stosowanie tego rachunku jest utrudnione, m.in. ze względu na realizację wieloaspektowego celu gospodarowania określonego specyficznymi cechami produkcji – jest to grunt wraz z drzewostanem. PGL LP prowadzą rachunkowość według zasad określonych w ustawie z dnia 29 września 1994 r. o rachunkowości[18] oraz rozporządzenia Rady Ministrów z dnia 29 września 1994 r. w sprawie szczegółowych zasad gospodarki finansowej w PGL LP[19].

W zakresie nieobjętym ustawą o rachunkowości LP stosują krajowe i Międzynarodowe Standardy Rachunkowości. Prowadzą działalność na zasadzie samodzielności finansowej i pokrywają koszty działalności z własnych przychodów. Dyrektor Generalny LP ustala dla wszystkich jednostek organizacyjnych LP politykę rachunkowości[20], której integralną częścią jest zakładowy plan kont oraz opis systemu informatycznego PGL LP.

red. L. Dziawgo, L. Patrzałek, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2016, nr 437, s. 396.

[18] Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2013 r. poz. 330 i 613).

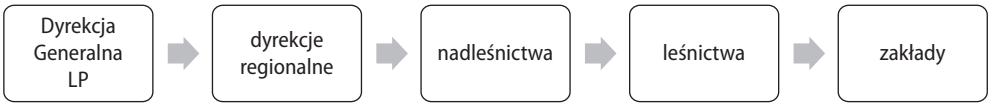
[19] Rozporządzenie Rady Ministrów z dnia 6 grudnia 1994 r. w sprawie szczegółowych zasad gospodarki finansowej w Państwowym Gospodarstwie Leśnym Lasy Państwowe.

[20] Art. 50 ustawy z dnia 28 września 1991 r. o lasach.

4. Rozwiązania zintegrowanego Systemu Informatycznego Lasów Państwowych w rachunkowości Lasów Państwowych

PGL LP nie należy do sektora przedsiębiorstw ani do sektora finansów publicznych. Jest szczególną organizacją działającą na podstawie odrębnych przepisów prawa dedykowanego tylko temu gospodarstwu. W grudniu 1990 r. Uchwałą Kolegium Lasów Państwowych zapadała decyzja w sprawie budowy Systemu Informatycznego Lasów Państwowych (SILP). To narzędzie informatyczne, które uwzględnia złożoność procesów gospodarczych na każdym poziomie zarządzania w PGL LP, co przedstawiono na rysunku 4.

Rysunek 4. Poziomy wykorzystywania SILP



Źródło: opracowanie własne.

W skład systemu SILP wchodzi aplikacja „Las" jako główny podsystem oraz inne zintegrowane ze sobą moduły. Integracja wewnętrzna systemu ewidencji aplikacji „Las" determinuje jednokrotne wprowadzenie każdego dowodu źródłowego w system. Dokument automatycznie staje się dostępny dla innych modułów. Integracja zewnętrzna systemu SILP umożliwia agregowanie informacji z niższych poziomów organizacyjnych na wyższe poziomy. Najważniejsze elementy tworzące system informatyczny LP przedstawiono w tabeli 1.

Do podstawowych funkcji realizowanych przez aplikację „Las", w zakresie podsystemu „Gospodarka Leśna", należą między innymi[21]:

- utrzymywanie danych o stanie lasu w formie corocznie aktualizowanych opisów taksacyjnych,
- inwentaryzacja posuszu,
- ewidencja występowania chorób i szkodników lasu, pożarów,

[21] A. Paszkiewicz, *System Informatyczny Lasów Państwowych*, w: *Podstawy rachunkowości i gospodarki finansowej w Lasach Państwowych*, red. A. Buraczewski, Wydawnictwo Uniwersytetu Przyrodniczego w Poznaniu, Poznań 2011, s. 252–255.

- ewidencja obiektów ekologicznych i rezerwatów,
- ewidencja szkód spowodowanych przez zwierzynę w uprawach leśnych,
- wspomaganie produkcji szkółkarskiej.

Tabela 1. Najważniejsze elementy tworzące system informatyczny LP

Lp.	Element systemu	Charakterystyka
1	Aplikacja „Las"	Zapewnia przetwarzanie danych transakcyjnych w ponad 450 jednostkach organizacyjnych Pracuje w architekturze rozproszonej
2	Rejestratory leśniczego	Są eksploatowane w ponad 5500 leśnictwach Zapewniają podstawową obsługę leśnictwa w zakresie rejestracji dokumentów źródłowych, w szczególności obrotu drewnem Zasilają tymi dokumentami system transakcyjny, funkcjonujący w 430 nadleśnictwach
3	Hurtownia danych	Agreguje dane przetwarzane w ramach aplikacji „Las" i aplikacji jej towarzyszących w poszczególnych jednostkach organizacyjnych LP oraz w centralnej bazie danych Portal INFOTAL udostępnia przetworzoną informację dla celów zarządczych i controllingowych na poszczególnych szczeblach organizacyjnych
4	Portal Leśno-Drzewny	Wspomaga proces sprzedaży drewna odbiorcom instytucjonalnym w formie rokowań internetowych Serwis internetowy e-Drewno stanowi elektroniczną platformę aukcyjną, za pomocą której zbywane są nadwyżki drewna niezagospodarowane poprzez Portal Leśno-Drzewny
5	Sieć rozległa Lasów Państwowych	Umożliwia zarządzanie rozległą infrastrukturą techniczną SILP, w szczególności w zakresie konserwacji i aktualizacji oprogramowania aplikacji „Las" – zapewnia możliwość bieżącego zasilania centralnej hurtowni danych informacjami z baz transakcyjnych jednostek.

Źródło: opracowanie własne na podstawie: A. Paszkiewicz, *System Informatyczny Lasów Państwowych*, w: *Podstawy rachunkowości i gospodarki finansowej w Lasach Państwowych*, red. A. Buraczewski, Wydawnictwo Uniwersytetu Przyrodniczego w Poznaniu, Poznań 2011, s. 246–247.

W ramach podsystemu „Gospodarka Leśna" funkcjonuje system planowania czynności gospodarczych, a system planów integruje informacje o przeszłych zdarzeniach gospodarczych w ujęciu ilościowym i wartościowym. Inne funkcje realizowane przez podsystemy SILP przedstawiono w tabeli 2.

Kolejnym podsystemem w ramach SILP jest podsystem „Finanse i Księgowość". W ramach ewidencji procesów gospodarczych odbywa się księgowanie na kontach wydatków i kosztów na podstawie dokumentów źródłowych własnych i obcych, wprowadzanych w tym systemie, jak również przejmowanie i ewidencjonowanie dokumentów kosztowych przekazywanych przez inne podsystemy (np. amortyzacja z podsystemu Infrastruktura). W tym podsystemie umieszczane są również dane

dotyczące wykonania kosztów i zadań rzeczowych, w powiązaniu z pozycjami planu. Podsystem „Finanse i Księgowość" pozwala na prowadzenie ewidencji pozabilansowej.

Tabela 2. Inne podsystemy i ich funkcje – system informatyczny SILP

Lp.	Podsystem systemu SILP	Wyszczególnienie
1	Gospodarka Towarowa	Ewidencja drewna Ewidencja stanu i obrotu produktami użytkowania ubocznego Ewidencjonowanie obrotu materiałami i towarami Fakturowanie Gospodarka łowiecka Inwentaryzacja
2	Kadry i Płace	Ewidencja danych o pracowniku Ewidencja czasu pracy Wykaz robót Karta deputatowa Dokumentacja płacowa
3	Infrastruktura	Obsługa inwentarza (środki trwałe, obwody łowieckie) Obsługa eksploatacji Obsługa rezerwacji* Obsługa naprawy Obsługa świadczeń stałych (dzierżawy, czynsze) Naliczanie amortyzacji

* Szerzej o funkcjach i zadaniach poszczególnych podsystemów, w tym o zadaniach w zakresie obsługi eksploatacji czy rezerwacji pisze A. Paszkiewicz, *System Informatyczny Lasów Państwowych*, w: *Podstawy rachunkowości i gospodarki finansowej w Lasach Państwowych*, red. A. Buraczewski, Wydawnictwo Uniwersytetu Przyrodniczego w Poznaniu, Poznań 2011, s. 252–253.

Źródło: opracowanie własne na podstawie: A. Paszkiewicz, *System Informatyczny Lasów Państwowych*, w: *Podstawy rachunkowości i gospodarki finansowej w Lasach Państwowych*, red. A. Buraczewski, Wydawnictwo Uniwersytetu Przyrodniczego w Poznaniu, Poznań 2011, s. 252–255.

Cechą, która odróżnia ten system od innych systemów informatycznych jest to, że zbudowano go wokół specyficznej dla PGL LP bazy danych opisów taksacyjnych[22]. Unikalną cechą tego systemu jest przeprowadzana corocznie aktualizacja bazy o zmiany wynikające z zaszłych zdarzeń gospodarczych.

System SILP spełnia wymogi w zakresie zaspokajania potrzeb informacyjnych użytkowników oraz pozwala na sporządzanie obligatoryjnych sprawozdań w zakresie

[22] Taksacja lasu (urządzanie lasu) — grupa czynności prac inwentaryzacyjnych polegająca na sporządzeniu opisu taksacyjnego wraz ze wstępnym oszacowaniem miąższości drzewostanów i określeniem wskazań gospodarczych. Kartograficznymi wynikami taksacji lasu są: mapa gospodarcza, mapy przeglądowe, mapa sytuacyjna. Opis taksacyjny sporządza się dla wszystkich gruntów pozostających w zarządzie nadleśnictwa, tj. lasów (gruntów: zalesionych, niezalesionych i związanych z gospodarką leśną) oraz gruntów nieleśnych, do których zalicza się również zadrzewione i zakrzewione. Szerzej: http://www.encyklopedialesna.pl, dostęp 24.10.2016.

prowadzonej rachunkowości finansowej. System ten na wyższych poziomach zarządzania jest jednak ubogi w mechanizm złożonego przetwarzania danych, dla funkcji rzeczywiście wspomagających zarządzanie (wielowariantowość, trendy, prognozy, różne przekroje kosztów).

5. Podsumowanie

W praktyce często utożsamiamy pojęcia danych i informacji. Informacje to wynik przetworzonych danych, które zostały odpowiednio zorganizowane oraz przedstawione. Przetwarzanie danych w informacje określane jest systemem informacyjnym[23]; system informatyczny to system, który składa się ze sprzętu komputerowego, oprogramowania, bazy danych, urządzeń i ośrodków łączności, ludzi i procedur. System informatyczny służy gromadzeniu, przetwarzaniu i generowaniu różnych informacji. W systemie rachunkowości gromadzone są dane szczególne, finansowe na potrzeby sprawozdawczości, raportowania wewnętrznego i zewnętrznego. SILP stanowi nowoczesne narzędzie informatyczne wykorzystywane w systemie całego gospodarstwa, a system rachunkowości jest jego ważnym elementem, gdyż gromadzi informacje.

Celem głównym opracowania była próba odpowiedź na pytanie badawcze: Czy SILP pozwala na generowanie i prezentowanie kompleksowej informacji o działalności Lasów Państwowych?

Wykorzystując takie metody badawcze, jak: studia literaturowe, analizę, wnioskowanie oraz dogłębną analizę źródeł prawa zewnętrznego oraz wewnętrznego Lasów Państwowych, stwierdzić należy, że SILP generuje dla PGL LP takie korzyści, jak:

- dostarcza wieloprzekrojowych informacji na potrzeby kierownictwa gospodarstwa, na różnych poziomach zarządzania,
- wykorzystuje mechanizmy, zapewniające bezpieczeństwo zasobów danych, poprzez:
  - wykorzystywanie funkcji GLOBAL,
  - dostęp do wybranych modułów tylko uprawnionych użytkowników oraz okresową ich weryfikację,
- obejmuje kanałami informacyjnymi wszystkie obszary PGL LP, takie jak: dyrekcje regionalne, nadleśnictwa, leśnictwa, a w tym, finanse, produkcję i zasoby ludzkie,

[23] Szerzej: A. Januszewski, *Funkcjonalność informatycznych systemów zarządzania*, t. 1, *Zintegrowane systemy translacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 22.

- podnosi wiarygodność informacji dzięki wprowadzaniu jej do systemu w miejscu powstawania, na przykład w nadleśnictwie,
- pozwala na oszczędność czasu z tytułu automatyzacji poszczególnych działań,
- generuje budżetowe, operacyjne analizy finansowe, raportowanie wewnętrzne,
- pozwala na zarządzanie strumieniami surowców, materiałów, usług, zleceń, w ramach całego gospodarstwa.

Należy podkreślić, iż w PGL LP poprzez wykorzystywanie SILP obserwuje się poprawę takich wskaźników, jak:

- poziom kosztów oferowania produktów,
- wydajność pracy,
- poziom kosztów osobowych,
- poziom kosztów produkcji.

Celem szczegółowym opracowania była próba odpowiedzi na pytanie: Czy stopień złożoności systemu SILP generuje szumy informatyczne? Współcześnie podmiotami rządzą informacje. Ich nadmiar generuje szumy informacyjne oraz wprowadza chaos w organizacji. SILP gromadzi wiele różnych informacji, a szum informacyjny determinuje takie negatywne zjawiska w nim, jak:

- pojawianie się zdezaktualizowanych informacji,
- przekazywanie informacji nieważnych z pominięciem tych ważnych i szczegółowych,
- subiektywizm interpretacji informacji, w związku z wiedzą lub jej brakiem u pracownika, który się tą informacją posługuje i przekazuje ją dalej,
- nadmiar informacji, których pracownicy nie są w stanie jednoznacznie zinterpretować, przetworzyć i przyswoić,
- negatywny wpływ na proces komunikacji w PGL LP,
- dodatkowy nakład pracy pracowników na wstępną selekcję danych – należy ocenić, czy dane, które do nas docierają, są w jakikolwiek sposób potrzebne, czy nie zawierają błędów,
- nadmiar informacji przekłada się bezpośrednio na trafność decyzji zarządczych.

Konkludując: SILP pozwala na generowanie i prezentowanie kompleksowej informacji o działalności Lasów Państwowych, jednocześnie stopień złożoności systemu SILP generuje szumy informatyczne, które mogą utrudniać dostarczanie rzetelnej bieżącej informacji na czas. W strategii PGL LP na lata 2014–2030 czytamy[24]:

[24] *Strategia Państwowego Gospodarstwa Leśnego Lasy Państwowe na lata 2014–2030*, Warszawa, grudzień 2013 r. www.lasy.gov.pl, dostęp 28.10.2016.

„Lasy Państwowe będą dążyć do równowagi, zapewniając możliwie wysokiej jakości wsparcie IT dla realizowanych procesów przy jednoczesnej wysokiej dbałości o racjonalność ponoszonych na nie wydatków (…) przejawami tego dążenia będą: optymalizacja zasobów i procesów informacyjnych".

PGL LP dostarcza użytkownikom wielu ważnych informacji finansowych i niefinansowych o działaniach i procesach wewnętrznych prowadzonej działalności produkcyjnej oraz pozaprodukcyjnej – jednocześnie ma świadomość nadmiaru informacji generowanych przez SILP i jest gotowe usprawniać procesy informatyczne, w tym niwelować szumy informacyjne.

Bibliografia

Akty normatywne

1. Rozporządzenie Rady Ministrów z dnia 6 grudnia 1994 r. w sprawie szczegółowych zasad gospodarki finansowej w Państwowym Gospodarstwie Leśnym Lasy Państwowe, Dz.U. z 1994 r. nr 134, poz. 692.
2. Ustawa z dnia 28 września 1991 r. o lasach (Dz.U. z 1991 r. nr 101, poz. 444 z późn. zm.)
3. Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2013 r. poz. 330 z późn. zm.).

Pozycje zwarte

1. Angryk R., *E-gospodarka*, w: *Inżynieria systemów informatycznych w e-gospodarce*, red. E. Kolbusz, W. Olejniczak, Z. Szyjewski, PWE, Warszawa 2005.
2. Bytniewski A., *Podsystem controlingu w ramach zintegrowanego systemu zarządzania jako źródło informacji na potrzeby rachunkowości zarządczej i controllingu*, w: *Rachunkowość a controlling*, red. E. Nowak, M. Kowalewski, M. Nieplowicz, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2016, nr 440.
3. Januszewski A., *Funkcjonalność informatycznych systemów zarządzania*, t. 1, *Zintegrowane systemy translacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.
4. Lulek A., *Od przeszłości do przyszłości – ewolucja rachunkowości i jej pojęcia*, w: *Dylematy i perspektywy rozwoju finansów i rachunkowości*, red. P. Szczypa, A. Zimny, Wydawnictwo Państwowej Wyższej Szkoły Zawodowej w Koninie, Konin 2017.
5. Łada M., *Automatyzacja procesów rachunkowości zarządczej*, w: *Rachunkowość a controlling*, red. E. Nowak, M. Kowalewski, M. Nieplowicz, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2016, nr 440.

6. Micherda B., *Funkcje i struktura współczesnej rachunkowości*, w: *Podstawy rachunkowości*, red. B. Micherda, Wydawnictwo Naukowe PWN, Warszawa 2005.
7. Nadolna B., *Dostosowanie informatycznych systemów rachunkowości do potrzeb zarządzania*, „Zeszyty Teoretyczne Rady Naukowej Stowarzyszenia Księgowych w Polsce" 2006, nr 35.
8. Paszkiewicz A., *System Informatyczny Lasów Państ*wowych, w: *Podstawy rachunkowości i gospodarki finansowej w Lasach Państwowych*, red. A. Buraczewski, Wydawnictwo Uniwersytetu Przyrodniczego w Poznaniu, Poznań 2011.
9. Roggal H., *Ekonomia zrównoważonego rozwoju*, Wydawnictwo Zysk i S-ka, Poznań 2010.
10. Sadowska B., *Strategia Państwowego Gospodarstwa Leśnego Lasy Państwowe a zrównoważony rozwój*, w: *Finanse na rzecz zrównoważonego rozwoju. Gospodarka – etyka – środowisko*, red. L. Dziawgo, L. Patrzałek, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2016, nr 437.
11. Sadowska B., *Znaczenie i warunki stosowania zintegrowanych systemów informatycznych w sferze budżetowej*, „Zeszyty Teoretyczne Rachunkowości" 2014, 76(132).

Artykuły i studia

1. Statut PGL LP, http://bip.lasy.gov.pl
2. Strategia PGL LP na lata 2014–2030, http://bip.lasy.gov.pl
3. Taksacja lasu, http://www.encyklopedialesna.pl

State Forests IT System. A Modern IT Tool Used in the Accounting System

Summary

An efficient operation of modern organisations depends on the degree of organisation and informatisation of business activities and processes. An integrated IT system of a business entity consists of many cooperating sub-systems whose role is to handle a complete scope of business events and operations as well as to provide a lot of updated and reliable information to meet the needs of internal and external users. The major aim of the study is to answer a research question: Does the State Forests IT System (SILP) allow for the generation and presentation of complex information about the operation of the State Forests? A detailed aim

is to answer another question: Does the complexity of the SILP system generate IT noise? The following research methods were used: the literature studies, analysis and conclusion drawing. It was also indispensable to thoroughly analyse the sources of external and internal law of the State Forests.

Keywords: State Forests, IT system, financial accounting sub-system, accounting

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 145–158

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

Jarosław Bogusław Wedler
Uniwersytet Szczeciński

Piotr Szczypa
Państwowa Wyższa Szkoła Zawodowa w Koninie

Czasoprzestrzeń rachunkowa kont wielostronnych jako podstawa oprogramowania finansowo-księgowego

Streszczenie

Użytkownicy systemów finansowo-księgowych nie otrzymują informacji w trybie *ex ante*, co niekorzystnie wpływa na proces podejmowania decyzji. Autorzy opracowania uważają, że aktualne rozwiązania informatyczne umożliwiają stworzenie oprogramowania finansowo-księgowego bazującego na koncepcji kont wielostronnych. Celem artykułu jest przedstawienie fundamentalnych założeń funkcjonowania kont wielostronnych, umożliwiających ewidencjonowanie zarówno przeszłych, jak i przyszłych zdarzeń gospodarczych, jako podstawy do nowego rodzaju oprogramowania finansowo-księgowego. Przyjęto następującą tezę: *czasoprzestrzeń rachunkowa kont wielostronnych stwarza możliwości nowatorskiego podejścia do konstruowania oprogramowania finansowo-księgowego, zapewniającego skuteczniejsze zaspokajanie potrzeb informacyjnych*. Autorzy wykorzystali metody indukcji i syntezy. Przeprowadzone badania dowodzą słuszności przyjętej tezy.

Słowa kluczowe: rachunkowość, konto wielostronne, czasoprzestrzeń rachunkowa, oprogramowanie finansowo-księgowe
Kod klasyfikacji JEL: M41

1. Wprowadzenie

Współczesny rozwój teoretycznej myśli rachunkowości ograniczony jest różnorodnością opisu zdarzeń gospodarczych i ich planowanych skutków. W podsystemie rachunkowości finansowej dominują zapisy na dwustronnych kontach księgowych z zastosowaniem reguły podwójnego zapisu. W podsystemie rachunkowości zarządczej większość zapisów jest pojedyncza i pozbawiona naturalnej kontroli poprawności ewidencjonowania. Zapisy księgowe z upływem czasu zostały przeniesione z nośnika papierowego do środowiska informatycznego. Zastosowanie informatycznych narzędzi w rachunkowości było naturalną konsekwencją zaspokajania potrzeb informacyjnych. Zdaniem I. Dziedziczaka informatyka dostarcza możliwości technologicznych, których urzeczywistnienie przynosi korzyści przedsiębiorstwu[1].

Podstawowymi zbiorami ewidencjonowania informacji są informatyczne bazy danych, funkcjonujące w sposób niejednorodny. Problem różnorodności zapisów *ex post* i *ex ante* rozwiązywany jest przez ukształtowanie struktury rekordów i zapytań. Jednak to rozwiązanie pozbawione jest naturalnej kontroli, wynikającej z reguły podwójnego zapisu. Reguła ta jest zastępowana przez sumy kontrolne i przekonanie, że algorytmy są właściwe i stabilne. Zastosowanie kont księgowych i reguły podwójnego zapisu do opisu planowanych zdarzeń gospodarczych stworzy teoretyczne podstawy do budowy oprogramowania finansowo-księgowego o nowych parametrach jakościowych i większej kontroli poprawności zapisów.

„Podniesienie jakości informacji sytemu rachunkowości nie sprowadza się do przyspieszenia jej obiegu i szczegółowości, gdyż powoduje to wzrost kosztów pozyskania informacji. Powinno się minimalizować je dla określonych potrzeb decyzyjnych. Należy również brać pod uwagę ewentualność, iż brak informacji może przynieść straty”[2]. Brak ewidencjonowania planowanych skutków zaistniałych zdarzeń gospodarczych może przynieść straty, wynikające z podejmowania nieoptymal-

[1] I. Dziedziczak, *Informatyka w rachunkowości*, PWE, Warszawa 1985, s. 5.
[2] Ibidem, s. 5.

nych decyzji zarządczych, oraz prowadzić do chybionego szacowania ryzyka. Dalej słusznie zauważa I. Dziedziczak, że jedno zdarzenie gospodarcze uzyskuje wielostronne niejako naświetlenie. Każde bowiem konto, na które odnosi się konkretną operację gospodarczą, a odnosi się ją zwykle na wiele kont, a zwłaszcza każda strona określonego konta wskazuje wybrany aspekt procesu odzwierciedlanego w rachunkowości. Operacja księgowa jest więc wieloaspektowym ujęciem zdarzenia gospodarczego[3]. Zdaniem autorów operacja księgowa powinna ujmować aspekt opisu planowanych skutków zdarzenia gospodarczego.

Zdaniem J.B. Wedlera, wieloaspektowe ujęcie zdarzenia gospodarczego na kontach księgowych pozwala na ewidencję samego zdarzenia i jego planowanych skutków. Konta wielostronne pozwalają na ujęcie zdarzenia gospodarczego retrospektywnie i prospektywnie z zachowaniem powiązań kont zgodnie z regułą podwójnego zapisu[4]. Ewidencjonowanie informacji o planowanych skutkach nie może być dowolne i obejmować wszystkich możliwych do przewidzenia zdarzeń. Według O. Johnsona, całość zdarzeń nigdy nie da się zmierzyć, a tylko pewne ich aspekty zaszłości można zaobserwować i zmierzyć[5]. Podobnie nie można przewidzieć, zmierzyć i opisać wszystkich możliwych do wystąpienia w przyszłości zdarzeń gospodarczych.

T. Peche[6] wskazywał na pragnienie S. Skrzywana[7] utworzenia dyscypliny związanej z całokształtem rachunku gospodarczego, obejmującego nie tylko rejestracje zaszłości, lecz także stwarzanie podstaw liczbowych dla kierownictwa przedsiębiorstwa do podejmowania decyzji. Zdaniem autorów niniejszego opracowania, ewidencjonowanie na kontach księgowych planowanych skutków zdarzeń gospodarczych stwarza podstawy liczbowe do podejmowania optymalnych decyzji zarządczych. Wiarygodność ewidencjonowanych liczb, opisujących planowane skutki zdarzeń gospodarczych, wynika z ich dostrzeżenia i pomiaru dokonanego w chwili ewidencjonowania danych o samym zdarzeniu gospodarczym oraz prawidłowego i wiarygodnego udokumentowania.

Celem artykułu jest przedstawienie fundamentalnych założeń funkcjonowania kont wielostronnych, umożliwiających ewidencjonowanie zarówno przeszłych, jak

---

[3] Ibidem, s. 9–10.

[4] J.B. Wedler, *Ograniczenia podwójnego zapisu na kontach księgowych w rachunkowości*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2015, nr 890, s. 149.

[5] O. Johnson, *Toward an „Events" Theory of Accounting*, „The Accounting Review" 1970, t. 45, nr 4, s. 641–653.

[6] T. Peche, *Podstawy współczesnej ewidencji gospodarczej*, PWN, Warszawa 1973, s. 20.

[7] S. Skrzywan, *Rachunkowość w przedsiębiorstwie przy gospodarce planowej. Cele i funkcje*, Prace Zakładu Rachunkowości SGH w Warszawie nr 1, Gospodarczy Instytut Wydawniczy, Warszawa 1948.

i planowanych zdarzeń gospodarczych, jako podstawy nowego rodzaju oprogramowania finansowo-księgowego. Przyjęto następującą tezę: *czasoprzestrzeń rachunkowa kont wielostronnych stwarza możliwości nowatorskiego podejścia do konstruowania oprogramowania finansowo-księgowego, zapewniającego skuteczniejsze zaspokajanie potrzeb informacyjnych*. Na potrzeby niniejszego artykułu wykorzystano metody indukcji i syntezy, użyte podczas formułowania wniosków. Wykorzystana literatura przedmiotu stanowi jedynie tło do prowadzonych rozważań, ponieważ koncepcja kont wielostronnych ma charakter innowacyjny i jest wynikiem badań prowadzonych obecnie tylko przez autorów. Dotychczas nie były prowadzone badania w zakresie kont wielostronnych i brak jest krajowej oraz międzynarodowej literatury innych autorów. Przedstawione w publikacji wyniki własnych badań stanowią część badań nad funkcjonowaniem i zastosowaniem wielostronnych kont księgowych w systemie rachunkowości i systemach informacyjnych podmiotów gospodarujących.

2. Zdarzenia i operacje gospodarcze

Powszechnie przyjmuje się, że ewidencji księgowej podlegają tylko zaistniałe i udokumentowane zjawiska gospodarcze. Jednak już przedstawione we wprowadzeniu treści świadczą, że możliwe jest ewidencjonowanie na kontach przyszłych skutków zdarzeń gospodarczych przy zachowaniu reguły podwójnego zapisu. Pogląd ten zaburza zakres definicyjny dwóch terminów, a mianowicie:

1) zdarzenia gospodarczego,
2) operacji gospodarczej.

Tradycyjnie pod pojęciem zdarzenia gospodarczego należy rozumieć ogół czynności dotyczących działalności gospodarczej podmiotu gospodarującego. Jednak nie wszystkie zdarzenia gospodarcze wywołują automatycznie zmiany w przychodach, kosztach i/lub składnikach bilansu. Niekiedy zmiany te następują w dalszym okresie po zaistnieniu zdarzenia gospodarczego, nie wywierają żadnych skutków dla systemu rachunkowości. Tradycyjnie przedmiotem szczególnego zainteresowania w rachunkowości są te zdarzenia gospodarcze, które wywołują bezpośrednie zmiany w składnikach rachunku zysków i strat i/lub bilansu. Taki rodzaj zdarzenia gospodarczego określany jest operacją gospodarczą. Zatem operacja gospodarcza to udokumentowane i podlegające ewidencji księgowej zdarzenie gospodarcze. Fakt podlegania ewidencji oznacza, że powoduje zmiany w składnikach bilansu (aktywa, pasywa) lub wpływa na wynik finansowy (zmiany w składnikach rachunku zysków

i strat). Z powyższego wynika, że zakres pojęcia „zdarzenie gospodarcze" jest szerszy od pojęcia „operacja gospodarcza"[8].

Prezentowane stanowisko autorów w niniejszym opracowaniu nie wpisuje się w przedstawioną interpretację podanych pojęć. Autorzy uważają, że pewien zakres zdarzeń gospodarczych umożliwia jednoczesne odniesienie na konta księgowe informacji o przeszłości i przyszłości (planowane skutki zdarzenia gospodarczego). W działalności podmiotów gospodarujących wstępują także zdarzenia gospodarcze, które dają podstawy do ewidencjonowania wyłącznie informacji dotyczących przyszłości. Istnieją też takie zdarzenia gospodarcze, które dają podstawy do ewidencji księgowej zarówno w trybie *ex post*, jak i *ex ante*. Zatem nawet przy założeniu możliwości ewidencjonowania zdarzeń przyszłych nie można postawić znaku równości między zdarzeniem gospodarczym a operacją gospodarczą. Autorzy na potrzeby artykułu rozważają wyłącznie takie zdarzenia, które podlegają ewidencji księgowej niezależnie od tego, czy niosą ze sobą informacje o przeszłości, czy przyszłości. W związku z tym przyjęto termin „zdarzenie gospodarcze" jako właściwe do rozważanego tematu, ponieważ ma w sobie pierwiastek odnoszący się do przyszłych skutków sytuacji, wynikającej z rozważanego zdarzenia gospodarczego.

3. Idea konta wielostronnego

Podstawowym urządzeniem księgowym jest dwustronne konto księgowe. Według Y. Ijria[9] rachunkowość jest nauką o mierzeniu i systemie pomiaru ekonomicznego. W podsystemie rachunkowości finansowej pomiar ekonomiczny ewidencjonowany jest na dwustronnych kontach księgowych z wykorzystaniem reguły podwójnego zapisu i sieci powiązań kont. W podsystemie rachunkowości zarządczej pomiar ekonomiczny planowanych skutków wcześniejszych zdarzeń gospodarczych nie jest ewidencjonowany na dwustronnych kontach księgowych, poza nielicznymi wyjątkami międzyokresowych kosztów czynnych i biernych czy też tworzonych rezerw, które to wyjątki stanową część podsystemu rachunkowości finansowej. W podsystemie rachunkowości zarządczej ewidencja dokonywana jest

[8] P. Szczypa, *Wpływ operacji gospodarczych na bilans i rachunek zysków i strat*, w: *Podstawy rachunkowości. Od teorii do praktyki*, red. P. Szczypa, CeDeWu, Warszawa 2016, s. 139–140.

[9] Y. Ijri, *Management Golas and Accounting for Control*, North – Holland Publishing Company, Amsterdam 1965, s. 56.

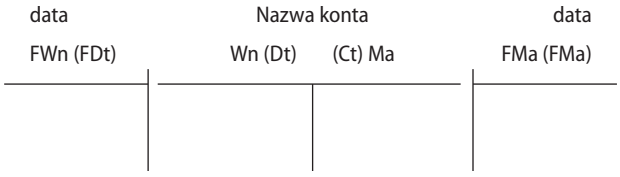
jako pojedynczy zapis bez zastosowania sieci powiązań wyników pomiaru ekonomicznego planowanych zdarzeń gospodarczych.

J.B. Wedler[10] zaproponował ewidencjonowanie wyników pomiaru ekonomicznego na kontach księgowych z zastosowaniem reguły podwójnego zapisu i sieci powiązań kont nie tylko zdarzeń gospodarczych, lecz także planowanych skutków wcześniej zaistniałych zdarzeń. Podstawowym założeniem idei konta wielostronnego jest ewidencjonowanie danych *ex post* i *ex ante* na dwustronnych kontach księgowych, które ze względu na rodzaj rejestrowanych danych różnie są oznaczane. W trybie *ex post* oznaczenie konta pozostaje bez zmian, w trybie *ex ante* konta wyróżnione są oznaczeniem FWn i FMa (FDb i FCt).

Zbiory kont *ex post* powiązane są ze zbiorem kont *ex ante* połączeniami korespondencji czasowej[11]. Rozwiązanie takie powoduje zwiększenie pojemności informacyjnej zawartej na kontach księgowych bez naruszania w istotny sposób obecnej teorii i reguł, a tym samym w sposób naturalny rozwija dotychczasową ewidencję księgową. Należy wskazać, że zwiększenie zdolności do gromadzenia informacji na kontach księgowych zmieni postrzeganie i pomiar zdarzeń. W wyniku zwiększenia ilości i jakości ewidencjonowanej informacji o przeszłości i przyszłości wzrośnie jakość i wiarygodność analiz finansowych oraz prognoz potrzebnych do podejmowania racjonalnych decyzji.

W sposób graficzny do celów edukacyjnych konto wielostronne można przedstawić w układzie podwójnego „T" (rysunek 1).

Rysunek 1. Konto wielostronne



Objaśnienie opisów:
data – określenie czasu przyszłego, w którym ma być dokonana operacja w kwocie określonej w FDt lub FCt (FWn lub FMa),
FDt – Future Debet (FWn) – zapis planowanego obciążenia konta lub zapisania w ciężar konta,
FCt – Future Credit (FMa) – zapis planowanego uznania konta lub zapisania na dobro konta.

Źródło: opracowanie własne na podstawie: J.B. Wedler, *Ograniczenia podwójnego zapisu na kontach księgowych w rachunkowości*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2015, nr 890, s. 147.

[10] J.B. Wedler, *Przesłanki i założenia funkcjonowania konta wielostronnego*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 300, s. 240.

[11] Ibidem, s. 242.

Zdaniem autorów wielostronne konta księgowe charakteryzuje uniwersalność, gdyż prowadzi się je osobno dla poszczególnych pozycji bilansu, kosztów i przychodów, ewidencjonujących pomiar ekonomiczny zaistniałych i planowanych zdarzeń.

Prowadzenie wielostronnych kont księgowych pozwala na ewidencjonowanie przyszłych zdarzeń, które nie są zgodne z planowanymi, a poprzez sieć powiązań korespondencji czasowej możliwe będzie dokonywanie odpowiednich zapisów korygujących[12]. Obecnie autorzy prowadzą prace badawcze i testy funkcji połączeń korespondencji czasowej wielostronnych kont księgowych. Wstępne wyniki potwierdzają zdolność kont i ich połączeń do budowy homogenicznej struktury informacyjnej, wykorzystującej w sieci powiązań danych regułę podwójnego zapisu.

Wielostronne konta księgowe umożliwiają scalenie podsystemów rachunkowości finansowej i zarządczej w jednorodny i spójny system rachunkowości. Do zalet tego rodzaju konta należy zaliczyć jego zdolność do odzwierciedlenia w rekordach baz danych, a tym samym struktura rekordów umożliwi uniwersalność i elastyczność zapytań. Właściwości te zwiększą przydatność systemów informatycznych w zakresie zwiększenia funkcjonalności oprogramowania finansowo-księgowego, a nawet możliwe będzie wyprzedzenie informacyjne w zakresie oczekiwanych zdarzeń.

W dotychczasowej praktyce i literaturze nie były stosowane i wykazywane podobne rozwiązania. Zdaniem autorów propozycja zastosowania w rachunkowości wielostronnego konta księgowego jest unikalnym i nowatorskim rozwiązaniem, mogącym w najbliższym czasie zmienić rozwiązania ewidencyjne w systemie rachunkowości.

4. Czasoprzestrzeń rachunkowa[13]

Z uwagi na zakres tematyczny artykułu autorzy prezentują wyniki swoich prac w formie zapisów na kontach księgowych w postaci macierzowej jako najbliższej idei odzwierciedlenia informatycznych baz danych. T. Peche[14] wskazywał na rozkwit metodologii bilansowej w postaci macierzowej, odnosząc się do prac W.W. Leontiewa i rozwoju informatyki, dzięki której standardowe procedury rachunku macierzowego

[12] Ibidem, s. 247–248.

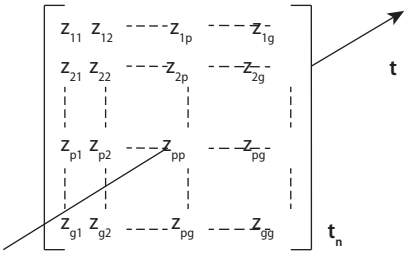
[13] Termin „czasoprzestrzeń rachunkowa" został zaproponowany przez J.B. Wedlera w opracowaniu: J.B. Wedler, *Struktura informacyjna czasoprzestrzeni rachunkowej*, w: *Współczesne wyzwania finansów i rachunkowości*, red. P. Szczypa, A. Zimny, Wydawnictwo PWSZ w Koninie, Konin 2017, s. 120.

[14] T. Peche, *Metody bilansowe w rachunkowości a systemy informacyjne w gospodarce narodowej*, PWN, Warszawa 1991, s. 56–59.

ułatwiają tworzenie zbiorów księgowych i manipulowanie nimi, a także obliczanie obrotów i sald.

Macierz ewidencjonującą na kontach sumę kwot zaistniałych zdarzeń gospodarczych w czasie t_n jednocześnie przynależnych do strony Wn jednego z kont i Ma drugiego, symboliczne oznaczamy $[z_{de}]$. Na rysunku 2 przedstawiono macierz $[z_{de}]$ dla t_n na osi czasu.

Rysunek 2. Płaszczyzna rachunkowa dla czasu t_n przedstawiona jako macierz kwadratowa



gdzie:
d, e = 1, 2, …, g, przy czym g = liczba kont.
t_n – czas ewidencjonowanych na kontach opisów zdarzeń gospodarczych.
Źródło: opracowanie własne na podstawie: I. Dziedziczak, *Informatyka w rachunkowości*, PWE, Warszawa 1985, s. 56.

Macierz $[z_{de}]$ tworzy płaszczyznę rachunkową[15] dla czasu t_n. Płaszczyzna rachunkowa może być, w celach edukacyjnych, przedstawiana również jako dendrytowe połączenia kont księgowych, zawierających ich stany po obydwu ich stronach, lub macierzy księgowań w konwencji W.W. Leontiewa czy L. Gomberga.

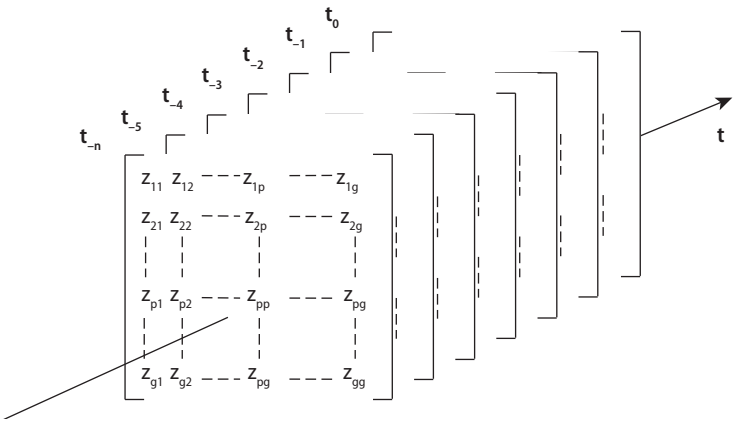
Wraz z upływem czasu następuje zapis kolejnych płaszczyzn rachunkowych zawierających macierze $[z_{de}]$ dla kolejnych czasów w interwałach przyjętych jako jednostki czasu rejestracji zmiany stanów kont. Zbiór płaszczyzn rachunkowych tworzy czasoprzestrzeń rachunkową, opisującą przeszłość podmiotu gospodarczego na kontach księgowych. Na rysunku 3 przedstawiono czasoprzestrzeń od czasu t_{-n} do czasu t_0 reprezentującego czas teraźniejszy.

W praktyce należy jednak przyjąć odmienne oznaczenie czasu dla poszczególnych płaszczyzn rachunkowych, a tym samym macierzy określających stany kont. Pierwsza płaszczyzna rachunkowa, opisująca powstanie jednostki gospodarczej,

[15] Termin „płaszczyzna rachunkowa" został zaproponowany przez J.B. Wedlera w opracowaniu: J.B. Wedler, *Struktura*…, op.cit., s. 117.

powinna być oznaczona jako t_0 i każda następna jako t_n do czasu ostatniego zapisu, ewidencjonującego likwidację jednostki. Przyjęcie takiego oznaczenia czasu związanego z kolejnymi płaszczyznami rachunkowymi jest bardziej adekwatne w praktycznym oznaczaniu czasu dla gromadzonych informacji w informatycznych bazach danych. Współcześnie na kontach księgowych ewidencjonowana jest informacja od powstania jednostki do czasu teraźniejszego (*ex post*), a tym samym w czasoprzestrzeni rachunkowej na kontach nie jest reprezentowana cała posiadana informacja, jak jest dostępna (*ex ante*). W niniejszej praca zaprezentowano tylko cząstkowe badania autorów w zakresie możliwości ewidencjonowania na kontach informacji o planowanych skutkach zaistniałych zdarzeń gospodarczych. Wstępne wyniki badań i testy autorów potwierdzają, że możliwe jest ewidencjonowanie na kontach księgowych informacji o przyszłości.

Rysunek 3. Czasoprzestrzeń rachunkowa opisu zdarzeń na kontach w ujęciu macierzowym



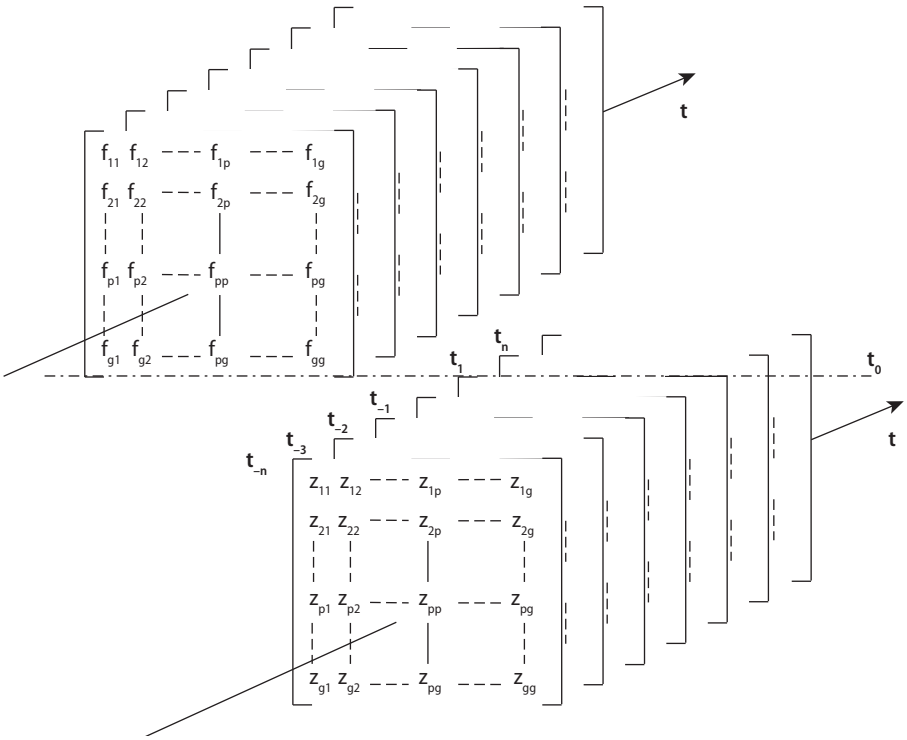
Źródło: opracowanie własne.

Przyjmując symboliczne oznaczenie macierzy opisującej na kontach planowane zdarzenia gospodarcze jako $[f_{de}]$, można przedstawić ewidencjonowanie planowanej przyszłości zbiorem płaszczyzn rachunkowych tworzących czasoprzestrzeń planowanych zdarzeń. Na rysunku 4 przedstawiono dwie czasoprzestrzenie rachunkowe ze zbiorami macierzy $[f_{de}]$ i $[z_{de}]$, zawierających informacje retrospektywne i prospektywne zapisane na kontach księgowych.

Wraz z upływem czasu następuje przyrost informacji o zaistniałych zdarzeniach gospodarczych (macierze $[z_{de}]$), którą można porównać z informacją

zaewidencjonowaną o planowanych zdarzeniach (macierze [f_{de}]). Na rysunku 3 sytuacja ta prezentowana jest przez płaszczyzny rachunkowe dla czasów od t_0 do t_2.

Rysunek 4. Czasoprzestrzenie rachunkowe *ex post* i *ex ante*

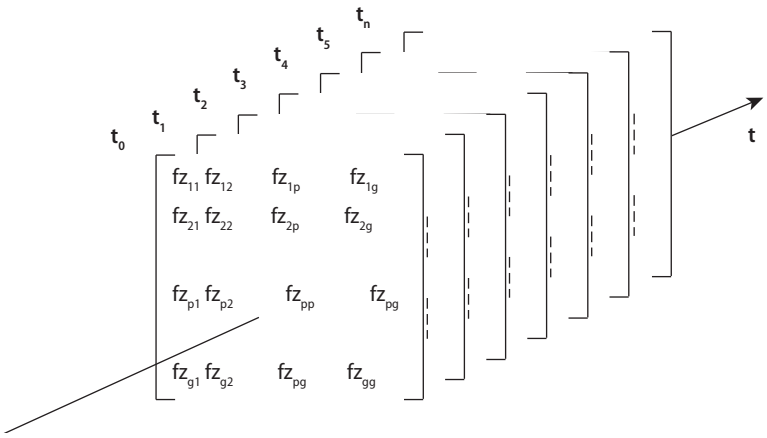


Źródło: opracowanie własne.

5. Podstawy nowego oprogramowania finansowo-księgowego

Zastosowanie wielostronnych kont księgowych pozwala stworzyć jedną czasoprzestrzeń rachunkową, zawierającą jeden zbiór macierzy opisujących zdarzenia gospodarcze i planowane zdarzenia. Symboliczne macierze [fz_{de}] opisują na wielostronnych kontach księgowych informacje *ex post* i *ex ante* o zdarzeniach gospodarczych i ich planowanych skutkach. Na rysunku 5 pokazano czasoprzestrzeń opisującą na kontach ich stany od powstania podmiotu gospodarującego w czasie t_0 do czasu likwidacji t_n.

Rysunek 5. Czasoprzestrzeń rachunkowa kont wielostronnych



Źródło: opracowanie własne.

Homogeniczna struktura czasoprzestrzeni rachunkowej wynika z ewidencjonowania informacji *ex post* i *ex ante* na kontach księgowych z zastosowaniem ich połączeń, zgodnie regułą podwójnego zapisu. Rozwiązanie takie daje nowe podstawy teoretyczne budowy informatycznych baz danych. Praktyczne wdrożenie koncepcji kont wielostronnych w rachunkowości będzie determinantą zdezaktualizowania twierdzenia T. Pechego, że funkcje kontrolne księgowości podwójnej, dbałość o prawidłowość rejestracji zaszłości i ich spójności, stosowanie procedur kontrolnych, aktualizacja zbiorów i ich zabezpieczenie są domeną administracji baz danych[16]. Według autorów czynności w sposób naturalny staną się kompetencjami księgowych w wyniku zastosowania koncepcji czasoprzestrzeni rachunkowej kont wielostronnych w ramach rozwiązań informatycznych oprogramowania finansowo-księgowego.

Według T. Pechego[17], „rachunkowość zdarzeniową" zapoczątkował G.H. Sorter[18], wskazujący potrzeby:

- dążenia do maksymalnego wzbogacenia informacyjnego fizycznego zapisu zdarzenia w bazach danych;

[16] T. Peche, *Metody…*, op.cit., s. 36–37.

[17] Ibidem, s. 36.

[18] G.H. Sorter, *An "Events" Approach to Basic Accounting Theory*, „The Accounting Review" 1969, nr 1, s. 12–19.

- dowolnego konstruowania informacji użytkowych w różnych strukturach logicznych przez zastosowanie odmiennych procedur, operujących na tych samych pierwotnych zapisach.

Organizując system rachunkowości przy użyciu jednego urządzenia księgowego (konto wielostronne) i jednej reguły powiązań kont – reguła podwójnego zapisu, tworzymy podstawy teoretyczne, pozwalające stworzyć rachunkowość zdarzeniową.

Słusznie zauważa I. Dziedziczak, że dalszy postęp zastosowania informatyki w rachunkowości wiedzie do wykorzystania w niej tego, co w informatyce nazywa się sztuczną inteligencją. Ekspertowe zastosowanie informatyki w rachunkowości sprowadza się w istocie do przeniesienia wiedzy i umiejętności do baz wiadomości, które wraz z bazą danych o faktach tworzą zbiory informacji, pozwalające reagować na sytuacje decyzyjne[19]. Możliwość porównania danych *ex post* i *ex ante* zgromadzonych w bazie danych [fz_{de}] oraz z bazą wiadomości otwiera drogę do tworzenia sztucznej inteligencji w oprogramowaniu finansowo-księgowym.

Należy zgodzić się z poglądem I. Dziedziczaka, że główny księgowy jest najlepiej zorientowanym ekonomistą w przedsiębiorstwie i z powodzeniem może wykonywać funkcje głównego ekonomisty, stając się maklerem informacji[20]. Należy dostrzec w tym miejscu wyniesienie na właściwe miejsce – postument – zawodu i pozycji księgowego w przedsiębiorstwie, który poza wiedzą archiwalną *ex post* będzie posiadał wiedzę o sytuacji jednostki w trybie *ex ante*. Pozwoli mu to prawidłowo doradzać decydentom.

6. Podsumowanie

Przedstawione treści skłaniają do stwierdzenia, że przyjęta teza jest prawdziwa, a jako główne wnioski końcowe należy wskazać wymienione niżej.

1. Rosnące zapotrzebowanie na informacje w trybie *ex ante* wymusza od podstawowego systemu informacyjnego, jakim jest rachunkowość, ewidencjonowanie na kontach księgowych nie tylko informacji o przeszłości, lecz także tych związanych z okresami przyszłymi. Taka sytuacja zmienia dotychczasową interpretację terminów: „operacja gospodarcza" i „zdarzenie gospodarcze".

[19] I. Dziedziczak, *Informatyka*…, op.cit., s. 14.

[20] Ibidem, s. 136.

2. Konto wielostronne umożliwia rejestrację przeszłych i przyszłych zdarzeń gospodarczych z zachowaniem zasady podwójnego zapisu.
3. Zastosowanie wielostronnych kont księgowych pozwala stworzyć jedną czasoprzestrzeń rachunkową, zawierającą jeden zbiór macierzy opisujących zdarzenia gospodarcze i planowane skutki tych zdarzeń.
4. Homogeniczna struktura czasoprzestrzeni rachunkowej stwarza nowe teoretyczne podstawy budowy informatycznych baz danych, stanowiących trzon oprogramowania finansowo-księgowego.
5. Oprogramowanie finansowo-księgowe, bazujące na koncepcji kont wielostronnych, dostarcza osobom decyzyjnym większy zakres informacji w porównaniu do dotychczasowego oprogramowania. Przewaga informacyjna związana jest z ewidencjonowaniem, przetwarzaniem i prezentowaniem informacji o przyszłości.
6. Stworzenie podstaw do budowy eksperckiego oprogramowania z wykorzystaniem sztucznej inteligencji.

Bibliografia

1. Dziedziczak I., *Informatyka w rachunkowości*, PWE, Warszawa 1985.
2. Ijri Y., *Management Golas and Accounting for Control*, North – Holland Publishing Company, Amsterdam 1965.
3. Johnson O., *Toward an «Events» Theory of Accounting*, „The Accounting Review" 1970, t. 45, nr 4.
4. Peche T., *Podstawy współczesnej ewidencji gospodarczej*, PWN, Warszawa 1973.
5. Peche T., *Metody bilansowe w rachunkowości a systemy informacyjne w gospodarce narodowej*, PWN, Warszawa 1991.
6. Skrzywan S., *Rachunkowość w przedsiębiorstwie przy gospodarce planowej. Cele i funkcje*, Prace Zakładu Rachunkowości SGH w Warszawie nr 1, Gospodarczy Instytut Wydawniczy, Warszawa 1948.
7. Sorter G.H., *An "Events" Approach to Basic Accounting Theory*, „The Accounting Review" 1969, nr 1.
8. Szczypa P., *Wpływ operacji gospodarczych na bilans i rachunek zysków i strat*, w: *Podstawy rachunkowości. Od teorii do praktyki*, red. P. Szczypa, CeDeWu, Warszawa 2016.
9. Wedler J.B., *Ograniczenia podwójnego zapisu na kontach księgowych w rachunkowości*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2015, nr 890.

10. Wedler J.B., *Przesłanki i założenia funkcjonowania konta wielostronnego*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 300.
11. Wedler J.B., *Struktura informacyjna czasoprzestrzeni rachunkowej*, w: *Współczesne wyzwania finansów i rachunkowości*, red. P. Szczypa, A. Zimny, Wydawnictwo PWSZ w Koninie, Konin 2017.

Accounting Spacetime of Multilateral Accounts as Basis for Financial-Accounting Software

Summary

The users of financial-accounting systems do not receive information in the ex-ante mode, which adversely affects the process of decision making. The authors of the article claim that that the current IT developments allow for the creation of financial-accounting software based on the concept of multilateral accounts. The aim of the study is to present fundamental assumptions of multilateral accounts allowing for the registering of past as well as future business events as the basis for a new kind of financial-accounting software. The following thesis is assumed in the study: *accounting spacetime of multilateral accounts allows for an innovative approach to the construction of the financial-accounting software to guarantee more effective satisfaction of IT needs.* The authors made use of the methods of induction and synthesis when working on the study. The conducted research proves that the assumed thesis was right.

Keywords: accounting, multilateral account, accounting spacetime, financial-accounting software

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 159–180

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

Piotr Wójtowicz
Uniwersytet Ekonomiczny w Krakowie

Czy trafność prognoz wyników finansowych spółek notowanych na GPW ma znaczenie?

Streszczenie

Celem artykułu jest udzielenie odpowiedzi na pytanie o rolę, jaką odgrywają analitycy giełdowi na polskim rynku kapitałowym wobec kształtowania wyniku finansowego przez zarządy spółek notowanych na Giełdzie Papierów Wartościowych w Warszawie. Narzędziem badawczym jest analiza empiryczna relacji między wynikami finansowymi prognozowanymi i raportowanymi. Badania przeprowadzono na próbie złożonej z 2723 obserwacji z lat 2002–2015 dotyczących 201 spółek. Różnice rozkładów prognoz wyniku netto oraz wyniku raportowanego wskazują, że trafność prognozy nie jest celem analityków ani zarządzających. Małe dodatnie błędy prognozy są bardziej prawdopodobne niż ujemne, co wskazuje na kształtowanie wyniku przez zarządy w celu osiągania wartości prognozowanych. Nie musi to być jednak sytuacja negatywna. Prognozy wyników mają rozkład nieświadczący o kształtowaniu, zatem analitycy-profesjonaliści mogą prognozować wyniki o charakterze permanentnym. Wobec tego zarząd, kształtując wynik, zapewnia wyższą jakość wyniku raportowanego niż w sytuacji, gdyby ten wynik był ujawniony neutralnie, co sugeruje się w Założeniach Koncepcyjnych MSR/MSSF.

Słowa kluczowe: prognozy wyników finansowych, błąd prognozy, trafność prognoz, jakość zysków, efektywność rynku
Kody klasyfikacji JEL: G10, G17, G14, G24, M41

1. Wprowadzenie

Wynik finansowy prezentowany w sprawozdaniach finansowych spółek giełdowych zajmuje czołową pozycję na liście kluczowych wskaźników efektywności (ang. *key performance indicators*) w sferze finansowej. Uczestnicy rynku są zainteresowani wynikiem zaprezentowanym w sprawozdaniu finansowym, ale także śledzą jego prognozy, formułowane w szczególności przez niezależnych analityków. Jest oczywiste, że wynik raportowany różni się od wartości prognozowanych, ale liczne badania pokazują, że rynek reaguje silnie na wartość i znak tej różnicy, zwanej w literaturze anglojęzycznej *earnings surprise*, czyli na wartość błędu prognozy *ex post*. Rynek amerykański reagował znacznym spadkiem wartości cen akcji w przypadku nawet niewielkich ujemnych błędów prognozy, czyli w sytuacji, gdy raportowana wartość wyniku finansowego była niższa niż prognozowana[1].

Powody, dla których zarządy spółek publicznych decydują się na kształtowanie wyniku finansowego (dalej: KWF), zostały już w literaturze przedmiotu usystematyzowane. Wyniki badań nie są w pełni jednoznaczne, jednak można stwierdzić, że zarządy mają powody, by kształtować wynik wokół trzech wartości progowych. Chodzi więc o znak wyniku finansowego (kształtowanie w celu unikania małych strat), wartość wyniku finansowego (kształtowanie w celu osiągania wyniku wyższego niż w poprzednim okresie, tzw. wygładzanie wyniku) oraz kształtowanie w celu osiągania wartości prognozowanych. Warunki kontraktów menedżerskich uzależniających wartość wynagrodzenia od wyniku spółki bądź cen akcji są podstawową zachętą do kształtowania. Zarządy „strategicznie" kształtują wynik, by osiągać wartości prognozowane przed kolejną emisją akcji. Koszt pozyskania kapitału obcego zależy od ryzyka oszacowanego przed jego dostawców, a więc w istocie także od wyników osiąganych przez spółkę. Przewidywalność wyników spółki ma znaczenie także dla biegłego rewidenta i wpływa na rodzaj opinii[2].

Z teorii wynika, że jeśli prognozy formułowane przez analityków są trafne, czyli analitykom udaje się przewiedzieć raportowany wynik finansowy, to błąd prognozy

[1] D.J. Skinner, R.G. Sloan, *Earnings Surprises, Growth Expectations, and Stock Returns or Don't Let an Earnings Torpedo Sink Your Portfolio*, „Review of Accounting Studies" 2002, vol. 7, iss. 2–3, s. 289–312; W. Kinney, D. Burgstahler, R. Martin, *Earnings Surprise "Materiality" as Measured by Stock Returns*, „Journal of Accounting Research" 2002, vol. 40, iss. 5, s. 1297–1329.

[2] A. Habib, J. Hansen, *Target Shooting: Review of Earnings Management around Earnings Benchmarks*, „Journal of Accounting Literature" 2008, vol. 27, s. 25–70.

powinien mieć rozkład symetryczny względem zera. Jednak na rynku amerykańskim rozkład ten był asymetryczny, w szczególności częstość występowania małych błędów dodatnich była większa niż małych ujemnych oraz rozkład miał lewy ogon grubszy niż prawy. Cytowani autorzy (dalej: AL2003) uważają, że było to spowodowane formułowaniem prognoz wolnych od kształtowania wyniku finansowego, gdy równocześnie wynik ujawniony był ukształtowany. Pośrednio oznaczałoby to, że analitycy nie dążą do formułowania prognoz trafnych, lecz o znacznej pojemności informacyjnej[3]. Równocześnie inni autorzy (dalej BE2003) podają, że rozkłady prognoz wyników oraz wyników raportowanych są podobne, jeśli chodzi o nieciągłość wokół zera, co jest w literaturze traktowane jako sygnał KWF w celu unikania strat. Wnioskują oni z przeprowadzonych badań, że analitycy doszukują się KWF, gdy ono nie występuje, oraz nie są w stanie prawidłowo usuwać jego skutków[4], jako że KWF jest trudne to uchwycenia nawet dla tak doświadczonych uczestników rynku jak analitycy[5]. Nowsze badania cytowanych wyżej autorów potwierdzają, jak sami twierdzą, wyniki wcześniejszych badań (BE2003). Według nich zarządzający dążą do unikania ujemnych błędów prognozy, zarówno kształtując wynik, jak i próbując wpływać na prognozy formułowane przez analityków[6].

Standardowy pogląd głosi więc, że KWF przez zarządy w celu osiągania wartości prognozowanych jest zjawiskiem negatywnym i szkodzącym interesom inwestorów. Jednak, zdaniem autora, nie musi takim być, a kluczowe znaczenie mieć będzie rola analityków i formułowanych przez nich prognoz. Jest bowiem możliwe, że prognozy są wolne, przynajmniej częściowo, od kształtowania wyników, a wtedy KWF w celu osiągania wartości prognozowanych może mieć pozytywne skutki dla inwestorów.

Celem artykułu jest poszukiwanie odpowiedzi na pytanie o rolę, jaką odgrywają analitycy giełdowi na polskim rynku kapitałowym, wobec kształtowania wyniku finansowego przez zarządy spółek notowanych na Giełdzie Papierów Wartościowych w Warszawie (GPW). Podstawowym narzędziem badawczym jest analiza empiryczna relacji między wynikami finansowymi prognozowanymi i raportowanymi. Badania

---

[3] J. Abarbanell, R. Lehavy, *Biased Forecasts or Biased Earnings? The Role of Reported Earnings in Explaining Apparent Bias and Over/Underreaction in Analysts' Earnings Forecasts*, „Journal of Accounting & Economics" 2003, vol. 36, iss. 1–3, s. 105–146.

[4] D. Burgstahler, M. Eames, *Earnings Management to Avoid Losses and Earnings Decreases: Are Analysts Fooled?*, „Contemporary Accounting Research" 2003, vol. 20, iss. 2, s. 253–294.

[5] P.E. Fischer, R.E. Verreechia, *Reporting Bias*, „Accounting Review" 2000, vol. 75, iss. 2, s. 229–245.

[6] D. Burgstahler, M. Eames, *Management of Earnings and Analysts' Forecasts to Achieve Zero and Small Positive Earnings Surprises*, „Journal of Business Finance & Accounting" 2006, vol. 33, iss. 5–6, s. 633–652.

przeprowadzono na próbie złożonej z 2723 obserwacji z lat 2002–2015 dotyczących 201 spółek. Uzyskane wyniki, podobne do AL2003, wskazują, że kształtowanie wyników raportowanych występuje, równocześnie prognozy nie są trafne. Sugeruje to, że uczestnicy rynku są raczej zainteresowani prognozami niosącymi nową informację. Jest to więc sytuacja przeciwna niż opisana w BE2003.

Dalsza część artykułu zorganizowana jest następująco: w punkcie 2 przedstawiono przegląd literatury, dotyczącej podejmowanej tu problematyki; w punkcie 3 cechy i znacznie GPW dla polskiej gospodarki; w punkcie 4. wyniki badań empirycznych; zaś w punkcie 5. dyskusję ich znaczenia, którą podsumowano zestawieniem najważniejszych wyników oraz przesłanek do dalszych badań.

2. Przegląd literatury

Informacje w prasie gospodarczej, a przede wszystkim badania naukowe, pokazują, że analitycy są nagradzani, jeśli ich prognozy są „prawidłowe", a rekomendacje skuteczne. Odnosząc się do kwestii „prawidłowości" prognozy, należy zwrócić uwagę na dwa możliwe kryteria oceny: trafność (ang. *accuracy*) oraz pojemność informacyjną (ang. *informativeness*). Trafność jest rozumiana jako różnica między prognozą a wynikiem raportowanym. W teorii prognozy, gdy mówi się o błędach prognozy, rozróżnia się dwa ich rodzaje. Błąd *ex ante* mierzy dokładności prognozy; jest szacowany przed upływem tego czasu, na który prognoza była ustalona. Błąd *ex post* mierzy trafność prognozy; jest obliczany po upływie czasu, na który prognoza była ustalona, czyli gdy znana jest realizacja zmiennej prognozowanej. Jeśli więc porównuje się wartości wyników finansowych prognozowane przez analityków z wartościami ze sprawozdań finansowych, to bada się trafność prognozy, choć z punktu widzenia uczestnika rynku kapitałowego dokładność może mieć większe znaczenie praktyczne w procesie decyzyjnym. Pojemność informacyjna wiąże się z użytecznością prognozy w procesie szacowania perspektyw rozwoju spółki[7]. Jest oczywiste, że trafna prognoza nie musi mieć znacznej pojemności informacyjnej

[7] J.C. Porter, M.A. Kraut, *Do Analysts Remove Earnings Management when Forecasting Earnings?*, „Academy of Accounting and Financial Studies Journal" 2013, vol. 17, iss. 2, s. 95–107. Warto dodać, że w teorii prognozy mówi się o dopuszczalności prognoz, co jest pojęciem bliskim pod względem treści. Prognoza jest dopuszczalna, gdy jest obdarzona przez jej odbiorcę stopniem zaufania wystarczającym do tego, by mogła być wykorzystana do celu, dla którego została ustalona. Dopuszczalność prognozy jest określona w tym samym czasie, w którym wyznacza się prognozę.

i *vice versa*. Elementarne znaczenie ma między innymi relacja między wartością skutków transakcji powtarzalnych i niepowtarzalnych prezentowanych w sprawozdaniu finansowym.

Z badań światowych – głównie amerykańskich – wynika, że inwestorzy reagują pozytywnie nie tylko na dodatnią wartość błędu prognozy, lecz także na fakt nawet nieznacznego przekroczenia wartości prognozowanych[8]. Sytuacja taka staje się zachętą do KWF właśnie w celu osiągania wartości prognozowanych, co było przedmiotem wielu badań, oprócz wspomnianych wyżej[9]. Kompleksowy przegląd literatury dotyczącej KWF w celu osiągania wartości progowych, także prognozowanych wartości zysków, znaleźć można w wielu publikacjach[10]. Na rynku amerykańskim od połowy lat 90. XX w. zarządy starają się przede wszystkim unikać ujemnych błędów prognozy kwartalnych zysków, zaś unikanie strat oraz zmniejszenia zysków tracą na znaczeniu. Rynek w USA nagradzał (karał) spółki, których wynik ujawniony był wyższy lub równy (niższy) od prognoz analityków bardziej niż w wypadku dwóch pozostałych progów[11].

---

[8] D. Matsumoto, *Management's Incentives to Avoid Negative Earnings Surprises*, „The Accounting Review" 2002, vol. 77, iss. 3, s. 483–514; E. Bartov, D. Givoly, C. Hayn, *The Rewards to Meeting or Beating Earnings Expectations*, „Journal of Accounting and Economics" 2002, vol. 33, iss. 2, s. 173–204; R. Kasznik, M. McNichols, *Does Meeting Earnings Expectations Matter? Evidence from Analyst Forecast Revisions and Share Prices*, „Journal of Accounting Research" 2002, vol. 40, iss. 3, s. 727–759; T. Lopez, L. Rees, *The Effect of Beating and Missing Analysts' Forecasts in the Information Content of Unexpected Earnings*, „Journal of Accounting, Auditing & Finance" 2002, vol. 17, iss. 2, s. 155–184; L. Rees, K. Sivaramakrishnan, *The Effect of Meeting or Beating Revenue Forecasts on the Association between Quarterly Returns and Earnings Forecast Errors*, „Contemporary Accounting Research" 2007, vol. 24, iss. 1, s. 259–290.

[9] J. Phillips, M. Pincus, S.O. Rego, *Earnings Management: New Evidence Based on Deferred Tax Expense*, „The Accounting Review" 2003, vol. 78, iss. 2, s. 491–521; J. Phillips, M. Pincus, S.O. Rego, H. Wan, *Decomposing Changes in Deferred Tax Assets and Liabilities to Isolate Earnings Management Activities*, „The Journal of the American Taxation Association" 2004, vol. 26, s. 43–66; M.M. Frank, S.O. Rego, *Do Managers Use the Valuation Allowance Account to Manage Earnings around Certain Earnings Targets?*, „The Journal of the American Taxation Association" 2006, vol. 28, iss. 1, s. 43–65.

[10] A. Habib, J. Hansen, *Target*…, op.cit.; M. Walker, *How Far Can We Trust Earnings Numbers? What Research Tells Us about Earnings Management*, „Accounting & Business Research" 2013, vol. 43, iss. 4, s. 445–481; S. Callao, J. Jarne, D. Wróblewski, *Debates and Studies on Earnings Management: a Geographical Perspective*, „Zeszyty Teoretyczne Rachunkowości" 2014, vol. 75(131), s. 145–169; S. Callao, J. Jarne, D. Wróblewski, *The Development of Earnings Management Research. A Review of Literature from Three Different Perspectives*, „Zeszyty Teoretyczne Rachunkowości" 2014, vol. 79(135), s. 135–177; S. Meisel, *Literature Review of Earnings Management – 1985–2014*, „Franklin Business & Law Journal" 2016, iss. 1, s. 91–144.

[11] L. Brown, M. Caylor, *A Temporal Analysis of Quarterly Earnings Thresholds: Propensities and Valuation Consequences*, „Accounting Review" 2005, vol. 80, iss. 2, s. 423–440.

Badania nad KWF w Europie są znacznie rzadsze niż w USA, a część publikacji była poświecona temu zjawisku, zwłaszcza w kontekście wprowadzenia w krajach Unii Europejskiej (UE) od 2005 roku MSR/MSSF jako systemu sprawozdawczego. Należy też zwrócić uwagę, że pokomunistyczne gospodarki rozwijające się stanowią swoistą *terra incognita*. KWF w Polsce do tej pory było przedmiotem zaledwie kilkunastu publikacji, głównie teoretycznych, które w niniejszej pracy nie są cytowane, jednak były omówione przez autora gdzie indziej[12].

Badania przeprowadzone na danych z krajów europejskich, na próbie z lat 1986–2001, a więc składającej się ze „starych" państw członkowskich UE, niezawierającej Polski, pokazały specyfikę rynków europejskich. Kształtowanie wyniku w celu osiągania wszystkich trzech wspomnianych wyżej wartości progowych odbywało się w stopniu większym niż w USA. Zakres kształtowania wewnątrz UE także był zróżnicowany: dążenie do unikania ujawniania strat oraz wygładzania wyniku finansowego było szczególnie silne w krajach, w których tradycyjnie funkcjonował system rachunkowości inkorporowany do systemu prawa, czyli typu *rules-based*[13]. Wyniki te pozwalają sformułować wniosek o zasadniczym wpływie uwarunkowań kulturowych i prawnych na funkcjonowanie systemu rachunkowości, który to wniosek znajduje potwierdzenie w nieco późniejszych badaniach[14] dotyczących związku między obowiązkowym zastosowaniem MSR/MSSF a KWF. Mimo stosunkowo nielicznej próby złożonej z danych z Australii, Francji i Wielkiej Brytanii pokazano, że zakres KWF nie zmniejszył się po przyjęciu MSR/MSSF, a we Francji istotnie wzrósł. Podobny wniosek wynika jednoznacznie z badań przeprowadzonych na próbie z lat 1995–2007 z Polski, przy czym dane wg MSR/MSSF dotyczyły tylko lat 2005–2007, czyli początkowego okresu ich obligatoryjnego funkcjonowania w polskiej praktyce[15]. Kolejne badania przeprowadzone na polskich danych

[12] P. Wójtowicz, *Earnings Management to Achieve Positive Earnings Surprises in Case of Medium Size Companies Listed in Poland*, „International Journal of Accounting and Economics Studies" 2015, vol. 3, iss. 2, s. 141–147.

[13] H. Daske, G. Gebhardt, S. McLeay, *The Distribution of Earnings Relative to Targets in the European Union*, „Accounting & Business Research" 2006, vol. 36 iss. 3, s. 137–167.

[14] T. Jeanjean, H. Stolowy, *Do Accounting Standards Matter? An Exploratory Analysis of Earnings Management before and after IFRS Adoption*, „Journal of Accounting & Public Policy" 2008, vol. 27, iss. 6, s. 480–494.

[15] P. Wójtowicz, *Wiarygodność sprawozdań finansowych wobec aktywnego kształtowania wyniku finansowego*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2010. Należy podkreślić, że najstarsze, a więc pionierskie, znane autorowi badania nad KWF w Polsce pochodzą z 2005 r. – K. Jackowicz, W. Kuryłek, *Unikanie raportowania strat przez banki komercyjne działające w Polsce*, „Studia i Prace Kolegium Zarządzania i Finansów Szkoły Głównej Handlowej" 2005, vol. 64, s. 63–84

z lat 2000–2010 sugerują, że wdrożenie MSR/MSSF nie wpłynęło istotnie na ograniczenie zakresu KWF w celu unikania ujawniania strat oraz wygładzania wyniku finansowego[16]. Oznacza to, że standaryzacja i harmonizacja systemu rachunkowości nie jest warunkiem wystarczającym do stworzenia „międzynarodowego języka biznesu" wysokiej jakości. Uwarunkowania funkcjonowania zarządzających i czynniki charakterystyczne dla krajów istotnie wpływają na jakość sprawozdań finansowych, także na KWF.

Znaczenie przyjęcia MSR/MSSF do praktyki sprawozdawczej w odniesieniu do KWF było podejmowane pośrednio także w innych badaniach, w których sprawdzano, czy zmiana ta wpłynęła pozytywnie na tzw. jakość zysków (ang. *earnings quality*) spółek notowanych na GPW. Jakość ta była wyrażona przez trwałość zysków (ang. *earnings persistence*) oraz wartość uznaniowych aktywów i kapitałów (ang. *accruals*). Wyniki wskazują na pozytywny, ale słaby związek między jakością zysków a wdrożeniem MSR/MSSF[17].

Zarządy spółek przyjmujących standardy międzynarodowe wcześnie i dobrowolnie robiły to w celu zwiększenia transparentności sprawozdań, a ostatecznie by zwrócić na siebie uwagę inwestorów (dostawców kapitału). Te zarządy, które zwlekały z zastosowaniem MSR/MSSF aż do momentu, w którym stało się to obowiązkowe, nie były zainteresowane zwiększeniem transparentności, zaś elastyczność nowego systemu wykorzystały do zwiększenia zakresu KWF, zwłaszcza wygładzania wyniku finansowego[18].

---

oraz P. Wójtowicz, *O malowaniu zysków na polskim rynku kapitałowym*, w: *Sprawozdawczość i rewizja finansowa w procesie poprawy bezpieczeństwa obrotu gospodarczego*, red. B. Micherda, Centrum Rozwoju i Promocji Akademii Ekonomicznej w Krakowie, Kraków 2005, s. 703–712. Ta pierwsza dotyczyła unikania ujawniania małych strat w polskich bankach komercyjnych, ta druga w spółkach notowanych na GPW. K. Jackowicz i L. Kozłowski w: *Zarządzanie wynikiem finansowym w bankach z Europy Środkowo-Wschodniej związane z progowymi wartościami rentowności*, „Master of Business Administration" 2010, vol. 5(114), s. 25–45 kontynuowali badania w odniesieniu do banków komercyjnych z państw Europy Centralnej, w tym Polski i wykazali dążenie do unikania małych strat, ale nie wygładzania wyniku.

[16] *Kształtowanie zysków podmiotów sprawozdawczych w Polsce. MSR/MSSF a ustawa o rachunkowości*, red. A. Piosik, C.H. Beck, Warszawa 2013.

[17] J. Michalak, H. Waniak-Michalak, P. Czajor, *Impact of Mandatory IFRS Implementation on Earnings Quality. Evidence From the Warsaw Stock Exchange*, „Zeszyty Teoretyczne Rachunkowości" 2012, vol. 68(124), s. 63–82.

[18] V. Capkun, D. Collins, T. Jeanjean, *The effect of IAS/IFRS Adoption on Earnings Management (Smoothing): A Closer Look at Competing Explanations*, „Journal of Accounting & Public Policy" 2016, vol. 35, iss. 4, s. 352–394.

Nowsze badania polskie dotyczą wielu aspektów KWF, przede wszystkim w celu unikania małych strat, znaczącej redukcji wyniku (ang. *big bath*) oraz jego wygładzania. W obszernej monografii zamieszczono kompleksowy przegląd zachęt i metod kształtowania w warunkach polskich, w odniesieniu zarówno do spółek notowanych na GPW, jak i nienotowanych. Przyjmuje się tam podzielany przez autora niniejszego artykułu pogląd o KWF jako zjawisku „szarym", to znaczy w zależności od okoliczności mogącym przynieść szkody bądź korzyści i to różnym interesariuszom przedsiębiorstwa[19]. Zarówno tam, jak i w kolejnej polskiej monografii nie podjęto problemu kształtowania wyniku w celu osiągania wartości prognozowanych przez analityków, choć zostały przeprowadzone kompleksowe badania determinant KWF w ujęciu międzynarodowym. Wynika z nich, że na zakres tego zjawiska mają wpływ zarówno czynniki charakteryzujące samą spółkę, uwarunkowania makroekonomiczne, jak i uwarunkowania kulturowe, instytucjonalne i prawne. KWF w tych badaniach było traktowane łącznie, bez rozróżniania celu (wartości progowej)[20]. Po raz kolejny okazało się więc, że o motywach i zakresie KWF decydują czynniki charakterystyczne dla grup spółek.

Kwestia kształtowania wyniku w celu unikania strat oraz jego wygładzania wydaje się być dobrze rozeznana w literaturze anglosaskiej oraz europejskiej, natomiast kształtowanie w celu osiągania wartości prognozowanych jest relatywnie słabo zbadane w Europie.

Badania dotyczące związku między KWF a pozostawaniem spółek w centrum zainteresowania niezależnych analityków wiązały się z tezą, że analitycy giełdowi, formułujący także prognozy wyników finansowych spółek notowanych, pełnią funkcję stróżów funkcjonowania rynku. Z badań wynika, że skuteczność analityków w tym zakresie rośnie wraz ze stopniem rozwoju systemu finansowego w państwie. W krajach wysoko rozwiniętych wzrost liczby analityków śledzących losy spółki i formułujących prognozy wiązał się ze zmniejszeniem zakresu KWF, nie obserwowano tej zależności w wypadku krajów słabo rozwiniętych[21].

---

[19] A. Piosik, *Kształtowanie wyniku finansowego przez podmioty sprawozdawcze w Polsce. Diagnoza dobrej i złej praktyki w rachunkowości*, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice 2016.

[20] K. Grabiński, *Determinanty kształtowania wyniku finansowego w teorii i praktyce europejskich spółek giełdowych*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2016.

[21] F. Degeorge, Y. Ding, T. Jeanjean, H. Stolowy, *Analyst Coverage, Earnings Management and Financial Development: An International Study*, „Journal of Accounting & Public Policy" 2013, vol. 32, iss. 1, s. 1–25.

Wstępne badania w zakresie KWF w celu osiągania wartości prognozowanych sugerują, że zarządy spółek z indeksu mWIG40 notowane na Giełdzie Papierów Wartościowych w Warszawie zachowują się podobnie, jak ich amerykańscy koledzy. Wyniki empiryczne wskazują, podobnie jak w wypadku AL2003, na ponadprzeciętną częstość występowania małych dodatnich błędów prognozy oraz gruby lewy ogon rozkładu[22]. Na tym tle pojawia się pytanie o przyczyny obserwowanego zjawiska. Czy analitycy faktycznie „widzą przez" KWF i potrafią oczyścić prognozy z jego skutków, w ten sposób zwiększając ich pojemność informacyjną, czy też może sytuacja jest wprost przeciwna, to znaczy dążą oni do zwiększenia trafności prognoz, być może kosztem informowania uczestników rynku. Podobny problem był przedmiotem badań empirycznych w USA[23], które raczej potwierdzają wyniki AL2003, a nie BE2003. Nie można jednak pomijać zasadniczych różnic między rynkiem polskim a amerykańskim.

3. Cechy charakterystyczne polskiej gospodarki i GPW

Pierwsza giełda papierów wartościowych w Polsce, poprzedniczka GPW, została otwarta w Warszawie w tym samym roku co giełda nowojorska, jednak okres jej dynamicznego rozwoju to ostatnie 25 lat (pierwsza sesja po przemianach końca lat 90. XX w. odbyła się 16 kwietnia 1991 r.). Zależność między kapitalizacją notowanych spółek krajowych a PKB dla Polski i wybranych krajów oraz ich grup przedstawiona jest w tabeli 1. Należy zwrócić uwagę na wzrost wartości tego wskaźnika w latach 2002–2007, potem gwałtowny spadek w roku 2008, spowodowany światowym kryzysem i charakterystyczny nie tylko dla Polski. Następnie w latach 2009–2010 obserwuje się wzrost, a w 2011 r. – zmniejszenie wartości. W latach 2012–2013 znów obserwuje się wzrost, potem w dwóch kolejnych latach w Polsce spadek o 10 p.p. w stosunku do 2013 r., ale np. w krajach OECD czy strefie euro – wzrost. Sytuacja ta może być spowodowana zmianami w systemie ubezpieczeń emerytalnych w Polsce, skutkującymi ograniczonym napływem kapitału przyszłych emerytów na giełdę.

[22] P. Wójtowicz, *Earnings…*, op.cit.

[23] J.C. Porter, M.A. Kraut, *Do Analysts…*, op.cit.

Tabela 1. Kapitalizacja rynkowa jako odsetek PKB w latach 2000–2015

Kraj/grupa krajów	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Czechy	12,6	15,6	22,6	25,7	28,6	36,5	17,4	–	–	–	–	–	–	–
Hiszpania	65,5	80,1	87,9	82,9	104,6	121,7	58,0	95,7	81,8	69,3	74,3	81,5	71,9	65,7
Francja	64,5	73,4	73,4	79,8	104,4	102,9	50,4	72,2	72,2	54,3	67,4	81,9	73,7	86,2
Luksemburg	105,3	127,8	146,0	138,6	189,7	330,0	120,8	208,5	193,2	115,2	125,6	127,3	97,4	81,6
Niemcy	33,0	43,1	42,4	42,0	54,5	61,2	29,6	37,8	41,8	31,5	42,0	51,7	44,9	51,1
Polska	**14,3**	**17,0**	**27,8**	**30,9**	**43,4**	**49,4**	**17,1**	**34,6**	**39,8**	**26,1**	**35,5**	**39,0**	**31,0**	**29,0**
Rumunia	5,4	5,7	14,4	15,9	20,4	17,9	7,3	7,8	8,5	7,6	–	–	–	–
Słowacja	109,0	114,1	163,0	148,8	285,5	8,0	5,4	5,7	4,7	5,5	5,0	4,9	–	–
Szwajcaria	203,5	206,6	210,7	230,3	282,5	267,0	159,6	197,3	211,5	156,5	185,4	224,9	213,3	228,6
Węgry	19,2	19,6	27,6	28,9	36,5	33,2	11,8	23,1	21,3	13,4	16,3	14,7	10,5	14,7
Włochy	37,7	39,2	43,9	43,1	52,8	48,7	21,8	30,0	25,2	19,0	23,2	28,9	27,5	–
USA	100,7	123,9	133,0	129,8	141,2	137,6	78,7	104,6	115,5	100,8	115,6	144,2	151,8	139,7
Centralna Europa	21,5	23,7	35,6	35,8	55,4	41,6	15,5	25,0	27,3	19,0	–	–	–	–
Kraje OECD	75,8	89,6	95,0	99,3	112,4	110,4	58,1	81,0	87,3	71,4	82,8	101,2	102,6	108,0
Unia Europejska	58,9	67,2	69,0	70,6	88,4	86,9	39,7	51,4	50,8	39,4	49,0	58,9	52,8	–
Strefa euro	49,5	57,0	59,8	60,5	78,6	80,3	36,4	53,1	52,3	40,7	49,9	60,2	54,2	65,7
Cały świat	74,6	85,8	90,4	93,4	107,1	114,9	56,6	83,0	86,8	67,4	77,7	88,7	91,6	97,9

Źródło: http://data.worldbank.org/indicator/CM.MKT.LCAP.GD.ZS, dostęp 17.10.2016.

Zjawisku zmniejszenia znaczenia roli giełdy w gospodarce zarząd GPW stara się przeciwdziałać między innymi przez wprowadzony w 2008 r. Program Wspierania Płynności. Elementem tego programu jest obowiązek prowadzenia przez emitenta sekcji relacji inwestorskich na własnej stronie internetowej oraz prezentowania informacji na tej stronie, zgodnie z zakresem oraz strukturą określonymi przez GPW.

Mimo rozlicznych trudności GPW jest największym rynkiem w całej Europie Centralnej i Wschodniej; ma cechy charakterystyczne, które pozwalają uznać ją za rynek jedyny w swoim rodzaju. Giełda w Polsce nie charakteryzuje się silnym związkiem ani z rynkami rozwiniętymi (np. niemieckim, brytyjskim), ani z rozwijającymi się (np. węgierskim, czeskim)[24]. Polska, 27 lat po rozpoczęciu znaczących reform mających na celu liberalizację gospodarki, jest średnio rozwiniętym systemem ekonomicznym o wielu cechach wspólnych z Włochami czy Hiszpanią. Biorąc pod uwagę stabilność finansów państwa i rankingi międzynarodowe długu publicznego, nawet przewyższa wspomniane kraje. Inflacja została opanowana (od lipca 2014 r. utrzymuje się niewielka deflacja), stopy procentowe są niskie i pozostają na stabilnym poziomie, rynek krajowy jest względnie duży, ponadto polscy producenci mają dostęp do rynków europejskich.

Wielu autorów zwraca uwagę, że jakość systemu rachunkowości i sprawozdań finansowych bardziej zależy od okoliczności, w których funkcjonują zarządy oraz skuteczności egzekwowania prawa niż od cech samego systemu rachunkowości[25]. Oznacza to, że bezpośrednie przenoszenie wyników badań z zagranicy na grunt polski jest nieuprawnione tym bardziej, że w perspektywie makroekonomicznej polska gospodarka także jest bardzo charakterystyczna. Cechy cykli finansowych w krajach rozwiniętych nie przystają do Polski. Zarówno długość, jak i amplituda cyklu kredytowego oraz cyklu akcji są inne niż w przypadku USA oraz Wielkiej Brytanii. W tych dwóch krajach o wysoko rozwiniętych rynkach kapitałowych cykle finansowe nie są zsynchronizowane z cyklem produkcji. W Polsce natomiast

[24] B. Égert, E. Kočenda, *Time-Varying Synchronization of European Stock Markets*, „Empirical Economics" 2011, vol. 40, iss. 2, s. 393–407; M. Adam, P. Bańbuła, M. Markun, *International Dependence and Contagion Across Asset Classes; the Case of Poland*, „Czech Journal of Economics and Finance" 2015, vol. 65, iss. 3, s. 254–270.

[25] D. Burgstahler, L. Hail, Ch. Leuz, *The Importance of Reporting Incentives: Earnings Management in European Private and Public Firms*, „The Accounting Review" 2006, 81, iss. 5, s. 983–1016; L. Hail, Ch. Leuz, P. Wysocki, *Global Accounting Convergence and the Potential Adoption of IFRS by the U.S. (Part I): Conceptual Underpinnings and Economic Analysis*, „Accounting Horizons" 2010, vol. 24, iss. 3, s. 355–394; R. Ball, A. Robin, J. Wu, *Incentives Versus Standards: Properties of Accounting Income in Four East Asian Countries*, „Journal of Accounting & Economics" 2003, vol. 36, iss. 1–3, s. 235.

rynek kapitałowy jest w fazie permanentnego rozwoju, a cykle finansowe są zbliżone do cyklu produkcji[26].

4. Wyniki badań empirycznych

Zwykle badania dotyczące KWF w celu osiągania wartości prognozowanych przez analityków prowadzone są z wykorzystaniem tzw. consensusu, czyli uśrednionej wartości prognoz wyników sformułowanych przez kilku analityków na dany dzień bilansowy. W warunkach polskich takie podejście jest znacznie utrudnione ze względu na ograniczony materiał empiryczny, czyli relatywnie mało dostępnych danych o prognozach. W tej sytuacji posłużenie się consensusem obliczonym samodzielnie lub pochodzącym np. z serwisu PAP powoduje, że analiza rozkładów empirycznych ma ograniczoną użyteczność. Z tego powodu w niniejszych badaniach posłużono się próbą złożoną z pojedynczych prognoz formułowanych przez analityków z wielu, w tym głównych, domów maklerskich, funkcjonujących na polskim rynku kapitałowym.

Wybór ten ma istotne znaczenie, bowiem zakłada się w ten sposób, że inwestorzy, czy szerzej – odbiorcy prognoz, w swoim procesie decyzyjnym posługują się nie tylko ich wartością średnią czy medianą na dzień bilansowy, lecz także indywidualnymi prognozami. Można się więc spodziewać, że analitycy dysponują zarówno informacjami publicznie dostępnymi na rynku, jak i prywatnymi, które komunikują właśnie przez prognozy[27]. Jeśli jednak inwestorzy posługują się consensusem, to korzystają tylko z informacji publicznych, bo średnia ma właściwości wygładzające. Posłużenie się pojedynczymi prognozami wiąże się z założeniem, że korzystają oni także z informacji prywatnych komunikowanych przez analityków.

Dane do analizy zaczerpnięto z serwisów internetowych http://www.inwestinfo.pl[28] oraz http://mojeinwestycje.interia.pl[29], na których gromadzone są prognozy wyników finansowych spółek giełdowych z biur maklerskich aktywnych na GPW. Z próby

[26] L. Lenart, M. Pipien, *Empirical Properties of the Credit and Equity Cycle within Almost Periodically Correlated Stochastic Processes – the Case of Poland, UK and USA*, „Central European Journal of Economic Modelling and Econometrics" 2015, iss. 7, s. 169–186.

[27] M.P. Kirk, D.A. Reppenhagen, J.W. Tucker, *Meeting individual analyst expectations*, „The Accounting Review" 2014, vol. 89, iss. 6, s. 2203–2231.

[28] http://www.inwestinfo.pl/rekomendacje-i-prognozy/rekomendacje/

[29] http://mojeinwestycje.interia.pl/gie/narzedzia/prognozy

wyłączono banki oraz instytucje finansowe i ubezpieczeniowe. Horyzont prognozy ograniczono do jednego roku obrotowego. Próba liczyła 2723 obserwacje dotyczące 201 spółek przygotowane przez 41 biur maklerskich za lata obrotowe 2002–2015. Dane o liczności próby zawarto w tabeli 2.

Tabela 2. Charakterystyka liczności próby

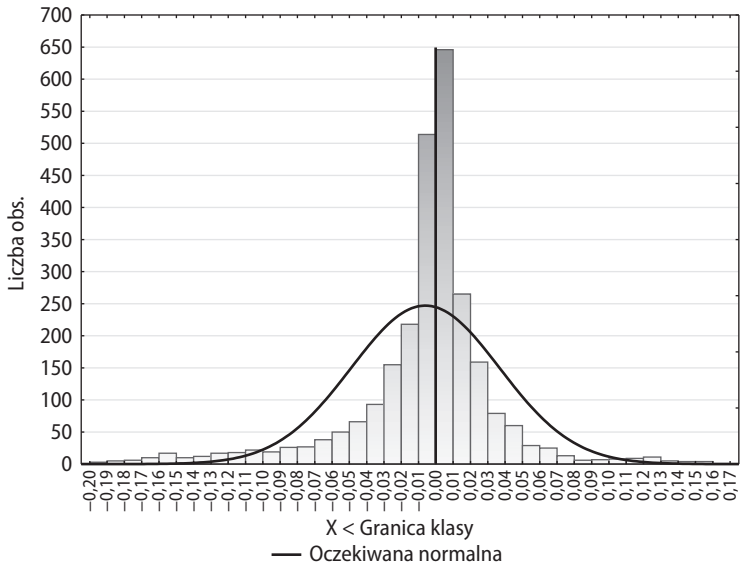
Wyszczególnienie	Średnia	Odch. std.	Min.	Max
Przekrój spółek: 201 spółek	13,5	16,6	1	80
Przekrój lat: 14 lat	194,5	185,7	23	597
Przekrój biur: 41 biur	66,4	103,9	1	379

Źródło: opracowanie własne.

Przedmiotem analizy uczyniono najpierw błąd prognozy *ex post*:

$$\textit{Błąd prognozy ex post} = \frac{\textit{Raportowany wynik netto} - \textit{Prognozowany wynik netto}}{\textit{Aktywa na początek roku}}$$

Rysunek 1. Histogram skalowanego błędu prognozy ***ex post***



Źródło: opracowanie własne.

Tabela 3. Statystyki opisowe analizowanych rozkładów

Wyszczególnienie	N	Średnia	Mediana	Odch. std.	Skośność	Kurtoza
Błąd prognozy *ex post*	2669	–0,0072	0,0000	0,0458	–1,3774	5,9871
Raportowany wynik netto	2672	0,0670	0,0548	0,0800	0,8724	3,4222
Prognoza wyniku netto	2669	0,0743	0,0552	0,0707	2,4348	9,7382
Raportowane przepł. pieniężne z dział. operac.	2669	0,0999	0,0936	0,0790	–0,0260	1,6106

Źródło: opracowanie własne.

Wszystkie statystyki opisowe podane w tabeli 3 dotyczą rozkładów analizowanych wielkości skalowanych wartością sumy bilansowej z początku roku. Średnia wartość błędu prognozy *ex post* jest ujemna –0,0072 ($p = 0{,}0000$ w jednostronnym teście *t*), co oznacza, że analitycy nie formułują prognoz trafnych, ponadto są nadmiernie optymistyczni, bowiem średnia wartość prognoz 0,0743 jest wyższa niż wyników raportowanych 0,0670. Wysoka, dodatnia wartość kurtozy 5,9871 dla błędu prognozy *ex post* świadczy o tym, że rozkład jest mocno skupiony wokół wartości centralnej i ma „grube ogony" (rysunek 1). Równocześnie ujemna wartość skośności –1,3774 informuje o lewostronnej asymetrii rozkładu, tzn. lewy ogon jest dłuższy i grubszy niż prawy. Sugeruje to, że analitycy nie prognozują trafnie wyników raportowanych, innymi słowy prognozy mogą być oczyszczone z kształtowania wyniku finansowego, bo wynik raportowany z całą pewnością jest ukształtowany. Przypuszczenie to może być zweryfikowane przez analizę osobno skalowanych zysków oraz skalowanych prognoz zysków, a także, kontrolnie, skalowanych przepływów z działalności operacyjnej.

Wartości statystyk opisowych podane w wierszach 3 i 4 tabeli 2 wskazują, że rozkłady są różne. Hipotezę o jednakowych wartościach średnich tych rozkładów zweryfikowano testem *t*, $p = 0{,}0128$. Testowano także założenie o jednorodności wariancji. Wartość $p = 0{,}0000$ w teście *F* z jednej strony wskazuje jednoznacznie na różnice rozkładów, z drugiej jest przesłanką do weryfikacji wyników testami nieparametrycznymi, wobec niespełnienia założeń teoretycznych stosowania testu *t*. Test serii Walda-Wolfowitza $p = 0{,}00$; test Kołmogorowa-Smirnowa dla dwóch prób $p < 0{,}001$; test *U* Manna-Whitneya $p = 0{,}0528$. Wyniki dwóch pierwszych testów wskazują na istotne różnice między rozkładami, test *U* daje wynik na granicy, jeśli przyjąć zwykle stosowany poziom istotności $\alpha = 0{,}05$.

Uzupełnieniem tej analizy jest ocena nieciągłości obu rozkładów wokół zera, traktowanej w literaturze jako przejaw kształtowania wyniku finansowego w celu unikania ujawniania małych strat. Posłużono się testem *BD* zaproponowanym przez Burgstahlera i Dicheva[30]:

$$BD = \frac{n_i - \frac{n_{i-1} + n_{i+1}}{2}}{\sqrt{N \times p_i \times (1 - p_i) + \frac{N \times (p_{i-1} + p_{i+1}) \times (1 - p_{i-1} - p_{i+1})}{4}}}$$

gdzie:
N – łączna liczba obserwacji,
n_i – liczba obserwacji w przedziale i,
p_i – prawdopodobieństwo, że obserwacja znajdzie się w przedziale i estymowana za pomocą częstości.

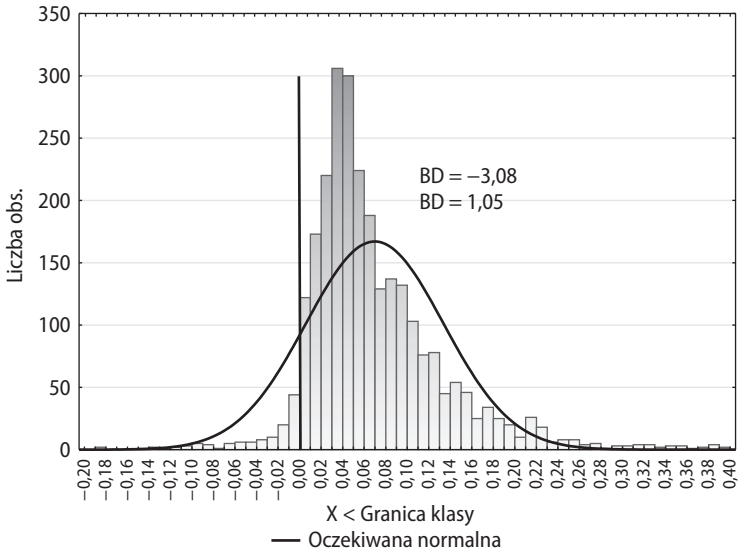
Metodyka ta została szczegółowo omówiona w monografii autora[31]. Należy wspomnieć, że wartość bezwzględna statystyki testowej większa od 3 bądź równa wskazuje na statystycznie istotną różnicę między licznością obserwowaną i oczekiwaną w przedziałach na lewo i prawo od zera, jeśli przyjąć poziom istotności $\alpha < 1\%$. Ze względów merytorycznych ważny jest również znak statystyki testowej, na lewo od zera wartość ujemna, na prawo dodatnia. Histogramy rozkładów zaprezentowano na rysunkach 2, 3 i 4. Na każdym z histogramów pionową linią oznaczono wartość zero.

Zgodnie z oczekiwaniami, rezultaty testu BD (por. rysunek 2) dla prognoz wyników netto wskazują na brak nieciągłości wokół zera, zatem prognozy nie są kształtowane w celu unikania małych strat. Potwierdza to domniemanie o prognozowaniu wyników nieukształtowanych. Trzeba jednak zwrócić uwagę, że analitycy przeszacowali liczbę prognoz małych strat, bowiem ich oczekiwana liczba w przedziale $-0{,}01 \leq x < 0$ wynosi 71, gdy rzeczywista wynosi 44. Równocześnie nieco nie doszacowali liczby małych zysków, bowiem liczność oczekiwana w przedziale $0 \leq x < 0{,}01$ wynosi 109, zaś rzeczywista 122.

[30] D.C. Burgstahler, I. Dichev, *Earnings Management to Avoid Earnings Decreases and Losses*, „Journal of Accounting and Economics" 1997, vol. 24, iss. 1, s. 99–126.

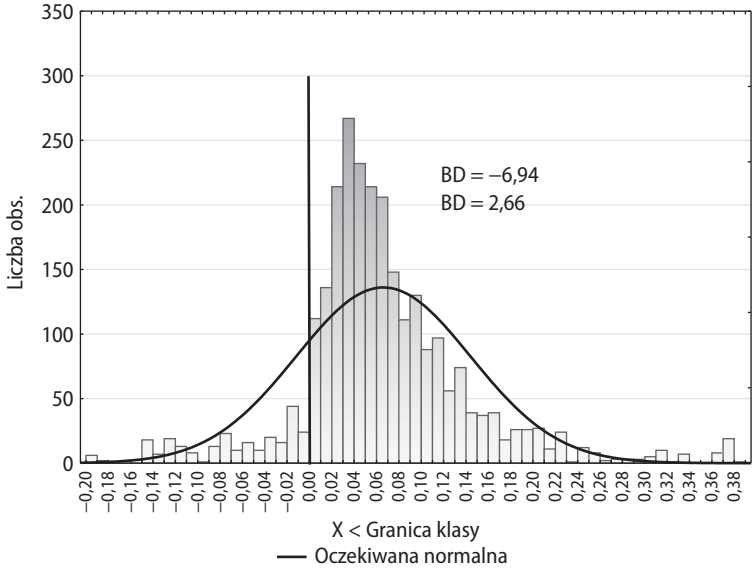
[31] P. Wójtowicz, *Wiarygodność*…, op.cit.

Rysunek 2. Histogram skalowanej prognozy wyniku netto i wartości statystyki BD



Źródło: opracowanie własne.

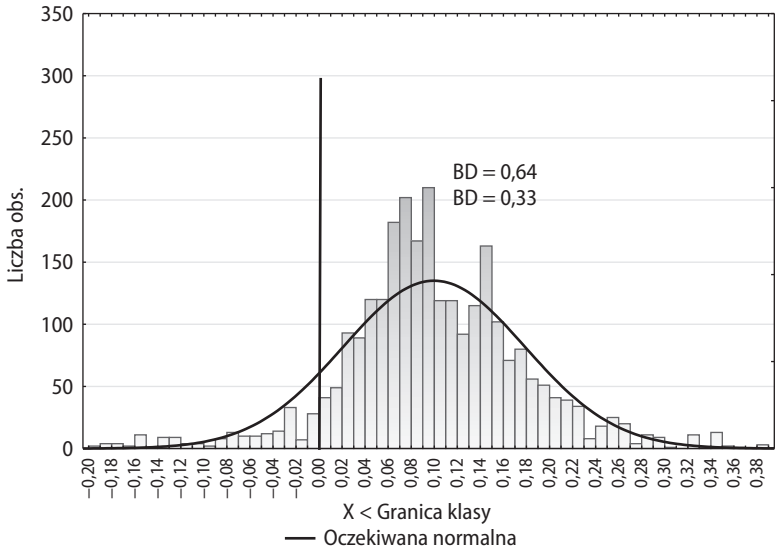
Rysunek 3. Histogram skalowanego raportowanego wyniku netto i wartości statystyki BD



Źródło: opracowanie własne.

Wyniki testu BD dla wyników raportowanych netto (por. rysunek 3) wskazują na ich kształtowanie w celu unikania ujawniania małych strat. Oczekiwana liczność w przedziale $-0{,}01 \leq x < 0$ wynosi 78, gdy rzeczywista 24, równocześnie liczność oczekiwana w przedziale $0 \leq x < 0{,}01$ wynosi 80, zaś rzeczywista 112.

Rysunek 4. Histogram skalowanych raportowanych przepływów pieniężnych z działalności operacyjnej i wartości statystyki BD



Źródło: opracowanie własne.

Analiza skalowanych przepływów z działalności operacyjnej (por. rysunek 4) nie wykazuje sygnałów kształtowania w celu unikania przepływów ujemnych (liczności rzeczywiste niemal równe oczekiwanym), co jest zgodnie z oczekiwaniami, bowiem przepływy można kształtować tylko przez bardzo trudne działania realne, a nie w obrębie polityki rachunkowości.

5. Podsumowanie

Stwierdzone zasadnicze różnice rozkładów prognoz wyniku netto oraz raportowanych wyników netto, a także ich charakterystyki wskazują, że trafność prognozy raczej nie jest stawką, o którą chodzi rozważanym uczestnikom gry rynkowej na GPW, czyli analitykom i zarządom. Jeśli wartość bezwzględna błędu prognozy

ex post jest duża, to jest prawdopodobne, że błąd ten jest ujemny, a więc wartość prognozy była większa niż wynik raportowany. Jeśli jednak wartość bezwzględna jest mała, to jest prawdopodobne, że wynik raportowany był wyższy niż prognoza. Oznacza to, że małe dodatnie błędy prognozy są bardziej prawdopodobne niż ujemne. Może to być uznane za sygnał świadczący o kształtowaniu wyniku przez zarządy w celu osiągania wartości prognozowanych.

Zdaniem autora, jest to sytuacja bardzo korzystna dla funkcjonowania rynku, biorąc pod uwagę całość uzyskanych tu wyników. Skoro bowiem wyniki są ukształtowane, zaś prognozy wyników mają inny rozkład, to znaczy, że analitycy, jako profesjonaliści, mogą „widzieć przez" kształtowanie wyniku. Innymi słowy prognozy mogą być wolne, przynajmniej częściowo, od skutków kształtowania typu memoriałowego. Są to więc wnioski podobne do AL2003, ale nie BE2003.

W tej sytuacji można wyobrazić sobie pewien scenariusz. Zarządy spółek podejmują próby kształtowania wyników w celu realizacji prognoz, a więc dodatkowej premii, którą rynek ewentualnie nagradza. Jednak wyniki prognozowane są wolne od krótkookresowego kształtowania, a więc mają charakter permanentny i lepiej niż wynik ukształtowany pokazują perspektywy rozwoju spółek. Ostatecznie zarząd, kształtując wynik w celu realizacji prognoz, zapewnia wyższą jakość wyniku raportowanego niż w sytuacji, gdyby ten wynik był ujawniony neutralnie, zgodnie z sugestiami zawartymi w Założeniach Koncepcyjnych MSR/MSSF. Uzyskano w ten sposób empiryczną koroborację wniosków sformułowanych wcześniej przez autora w studium teoretycznym[32].

Przedstawiony scenariusz, jakkolwiek może być prawdziwy, musi być zweryfikowany w wyniku dalszych badań empirycznych. Konieczne jest więc stwierdzenie, czy polski rynek GPW nagradza (karze) osiąganie (brak osiągania) wyników prognozowanych. Na tym tle nadal jest aktualne pytanie o to, czy rynek oczekuje prognoz trafnych (jak się wydaje: niekoniecznie), czy też o znacznej pojemności informacyjnej. Wyniki tych badań mogą wskazać na niezwykle istotną rolę analityków pracujących na giełdzie, bo w istocie mogą oni pełnić funkcję strażników (ang. *gatekeepers*) przyczyniających się do wzrostu jakości zysków i wiarygodności sprawozdań, a więc efektywności informacyjnej rynku.

[32] P. Wójtowicz, *Neutralność jako ważna cecha sprawozdania finansowego?*, w: *Polityka rachunkowości a kształtowanie wyniku finansowego*, red. A. Kostur, J. Pfaff, „Studia Ekonomiczne, Zeszyty Naukowe Wydziałowe Uniwersytetu Ekonomicznego w Katowicach" 2014, nr 201, s. 424–431.

Bibliografia

Wydawnictwa zwarte

1. Grabiński K., *Determinanty kształtowania wyniku finansowego w teorii i praktyce europejskich spółek giełdowych*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2016.
2. *Kształtowanie zysków podmiotów sprawozdawczych w Polsce. MSR/MSSF a ustawa o rachunkowości*, red. A. Piosik, C.H. Beck, Warszawa 2013.
3. Piosik A., *Kształtowanie wyniku finansowego przez podmioty sprawozdawcze w Polsce. Diagnoza dobrej i złej praktyki w rachunkowości*, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice 2016.
4. Wójtowicz P., *Wiarygodność sprawozdań finansowych wobec aktywnego kształtowania wyniku finansowego*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2010.

Artykuły

1. Abarbanell J., Lehavy R., *Biased Forecasts or Biased Earnings? The Role of Reported Earnings in Explaining Apparent Bias and Over/Underreaction in Analysts' Earnings Forecasts*, „Journal of Accounting & Economics" 2003, vol. 36, iss. 1–3.
2. Adam M., Bańbuła P., Markun M., *International Dependence and Contagion Across Asset Classes; the Case of Poland*, „Czech Journal of Economics and Finance" 2015, vol. 65, iss. 3.
3. Ball R., Robin A., Wu J., *Incentives Versus Standards: Properties of Accounting Income in Four East Asian Countries*, „Journal of Accounting & Economics" 2003, vol. 36 iss. 1–3.
4. Bartov E., Givoly D., Hayn C., *The Rewards to Meeting or Beating Earnings Expectations*, „Journal of Accounting and Economics" 2002, vol. 33, iss. 2.
5. Brown L., Caylor M., *A Temporal Analysis of Quarterly Earnings Thresholds: Propensities and Valuation Consequences*, „Accounting Review" 2005, vol. 80, iss. 2.
6. Burgstahler D.C., Dichev I., *Earnings Management to Avoid Earnings Decreases and Losses*, „Journal of Accounting and Economics" 1997, vol. 24, iss. 1.
7. Burgstahler D., Eames M., *Earnings Management to Avoid Losses and Earnings Decreases: Are Analysts Fooled?*, „Contemporary Accounting Research" 2003, vol. 20, iss. 2.
8. Burgstahler D., Eames M., *Management of Earnings and Analysts' Forecasts to Achieve Zero and Small Positive Earnings Surprises*, „Journal of Business Finance & Accounting" 2006, vol. 33, iss. 5–6.

9. Burgstahler D., Hail L., Leuz Ch., *The Importance of Reporting Incentives: Earnings Management in European Private and Public Firms*, „The Accounting Review" 2006 81, iss. 5.
10. Callao S., Jarne J., Wróblewski D., *Debates and Studies on Earnings Management: A Geographical Perspective*, „Zeszyty Teoretyczne Rachunkowości" 2014, vol. 75(131).
11. Callao S., Jarne J., Wróblewski D., *The Development of Earnings Management Research. A Review of Literature From Three Different Perspectives*, „Zeszyty Teoretyczne Rachunkowości" 2014, vol. 79(135).
12. Canace T.G., Salzsieder L., *The Timing of Asset Purchases to Achieve Earnings Thresholds*, „Journal of Management Accounting Research" 2016, vol. 28, iss. 1.
13. Capkun V., Collins D., Jeanjean T., *The Effect of IAS/IFRS Adoption on Earnings Management (Smoothing): A Closer Look at Competing Explanations*, „Journal of Accounting & Public Policy" 2016, vol. 35, iss. 4.
14. Daske H., Gebhardt G., McLeay S., *The Distribution of Earnings Relative to Targets in the European Union*, „Accounting & Business Research" 2006, vol. 36 iss. 3.
15. Degeorge F., Ding Y., Jeanjean T., Stolowy H., *Analyst Coverage, Earnings Management and Financial Development: An International Study*, „Journal of Accounting & Public Policy" 2013, vol. 32, iss. 1.
16. Égert B., Kočenda E., *Time-varying synchronization of European stock markets*, „Empirical Economics" 2011, vol. 40, iss. 2.
17. Fischer P.E., Verreechia R.E., *Reporting Bias*, „Accounting Review" 2000, vol. 75, iss. 2.
18. Frank M.M., Rego S.O., *Do Managers Use the Valuation Allowance Account to Manage Earnings around Certain Earnings Targets?*, „The Journal of the American Taxation Association" 2006, vol. 28, iss. 1.
19. Habib A., Hansen J., *Target Shooting: Review of Earnings Management around Earnings Benchmarks*, „Journal of Accounting Literature" 2008, vol. 27.
20. Hail L., Leuz Ch., Wysocki P., *Global Accounting Convergence and the Potential Adoption of IFRS by the U.S. (Part I): Conceptual Underpinnings and Economic Analysis*, „Accounting Horizons" 2010, vol. 24, iss. 3.
21. Jackowicz K., Kozłowski L., *Zarządzanie wynikiem finansowym w bankach z Europy Środkowo-Wschodniej związane z progowymi wartościami rentowności*, „Master of Business Administration" 2010, vol. 5(114).
22. Jackowicz K., Kuryłek W., *Unikanie raportowania strat przez banki komercyjne działające w Polsce*, „Studia i Prace Kolegium Zarządzania i Finansów Szkoły Głównej Handlowej" 2005, vol. 64.
23. Jeanjean T., Stolowy H., *Do Accounting Standards Matter? An Exploratory Analysis of Earnings Management Before and After IFRS Adoption*, „Journal of Accounting & Public Policy" 2008, vol. 27, iss. 6.

24. Kasznik R., McNichols M., *Does Meeting Earnings Expectations Matter? Evidence from Analyst Forecast Revisions and Share Prices*, „Journal of Accounting Research" 2002, vol. 40, iss. 3.
25. Kinney W., Burgstahler D., Martin R, *Earnings Surprise "Materiality" as Measured by Stock Returns*, „Journal of Accounting Research" 2002, vol. 40, iss. 5.
26. Kirk M.P., Reppenhagen D.A., Tucker J.W., *Meeting Individual Analyst Expectations*, „The Accounting Review" 2014, vol. 89, iss. 6.
27. Lenart L., Pipien M., *Empirical Properties of the Credit and Equity Cycle within Almost Periodically Correlated Stochastic Processes — the Case of Poland, UK and USA*, „Central European Journal of Economic Modelling and Econometrics" 2015, iss. 7.
28. Lopez T., Rees L., *The Effect of Beating and Missing Analysts' Forecasts in the Information Content of Unexpected Earnings*, „Journal of Accounting, Auditing & Finance" 2002, vol. 17, iss. 2.
29. Matsumoto D., *Management's Incentives to Avoid Negative Earnings Surprises*, „The Accounting Review" 2002, vol. 77, iss. 3.
30. Meisel S., *Literature Review of Earnings Management — 1985–2014*, „Franklin Business & Law Journal" 2016, iss. 1.
31. Michalak J., Waniak-Michalak H., Czajor P., *Impact of Mandatory IFRS Implementation on Earnings Quality. Evidence From the Warsaw Stock Exchange*, „Zeszyty Teoretyczne Rachunkowości" 2012, vol. 68(124).
32. Phillips J., Pincus M., Rego S.O., *Earnings Management: New Evidence Based on Deferred Tax Expense*, „The Accounting Review" 2003, vol. 78, iss. 2.
33. Phillips J., Pincus M., Rego S.O., Wan H., *Decomposing Changes in Deferred Tax Assets and Liabilities to Isolate Earnings Management Activities*, „The Journal of the American Taxation Association" 2004, vol. 26.
34. Porter J.C., Kraut M.A., *Do Analysts Remove Earnings Management when Forecasting Earnings?*, „Academy of Accounting and Financial Studies Journal" 2013, vol. 17, iss. 2.
35. Rees L., Sivaramakrishnan K., *The Effect of Meeting or Beating Revenue Forecasts on the Association between Quarterly Returns and Earnings Forecast Errors*, „Contemporary Accounting Research" 2007, vol. 24, iss. 1.
36. Skinner D.J., Sloan R.G., *Earnings Surprises, Growth Expectations, and Stock Returns or Don't Let an Earnings Torpedo Sink Your Portfolio*, „Review of Accounting Studies" 2002, vol. 7, iss. 2–3.
37. Walker M., *How Far Can We Trust Earnings Numbers? What Research Tells Us about Earnings Management*, „Accounting & Business Research" 2013, vol. 43, iss. 4.
38. Wójtowicz P., *O malowaniu zysków na polskim rynku kapitałowym*, w: *Sprawozdawczość i rewizja finansowa w procesie poprawy bezpieczeństwa obrotu gospodarczego*, red. B. Micherda, Centrum Rozwoju i Promocji Akademii Ekonomicznej w Krakowie, Kraków 2005.

39. Wójtowicz P., *Neutralność jako ważna cecha sprawozdania finansowego?*, w: *Polityka rachunkowości a kształtowanie wyniku finansowego*, red. A. Kostur, J. Pfaff, „Studia Ekonomiczne, Zeszyty Naukowe Wydziałowe Uniwersytetu Ekonomicznego w Katowicach" 2014, nr 201.
40. Wójtowicz P., *Earnings Management to Achieve Positive Earnings Surprises in Case of Medium Size Companies Listed in Poland*, „International Journal of Accounting and Economics Studies" 2015, vol. 3, iss. 2.

Źródła internetowe

1. http://data.worldbank.org/indicator/CM.MKT.LCAP.GD.ZS
2. http://mojeinwestycje.interia.pl/gie/narzedzia/prognozy
3. http://www.inwestinfo.pl/rekomendacje-i-prognozy/rekomendacje

Is the Accuracy of Forecasts of Financial Results of Public Companies Listed on the Warsaw Stock Exchange significant?

Summary

The aim of this article is to answer a question about a role played by stock market analysts on the Polish capital market in relation to the development of financial result by the managements of companies listed on the Warsaw Stock Exchange. The research tool is an empirical analysis of relations between the forecast and reported financial results. A survey conducted on a sample consisting of 2,723 observations in 2002–2015 referring to 201 companies. The differences of forecast distribution of the net result reported result indicate that the forecast accuracy is not the goal of analysts or managers. Small positive forecast errors are more likely than negative, which indicates affecting the result by managements in order to achieve the forecast values. It does not have to be a negative situation. The forecasts of results have a distribution which does not indicate any impact, so professional analysts may forecast results of permanent character. Due to this, the management when affecting the result, ensures a higher quality of the reported result than in the situation when this result is revealed neutrally, which is suggested in the Conceptual Assumptions of IRS/IFRS.

Keywords: financial results forecasts, forecast error, forecast accuracy, profit quality, market efficiency

STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 181–201

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

Michał Comporek
Zakład Analizy i Strategii Przedsiębiorstwa
Uniwersytet Łódzki

Naruszanie obowiązku informacyjnego przez emitentów papierów wartościowych w świetle sankcji KNF

Streszczenie

Jedną z kompetencji przysługujących Komisji Nadzoru Finansowego jest troska o przejrzystość w zakresie zarządzania spółkami, których akcje są przedmiotem obrotu na Głównym Rynku GPW w Warszawie. Wyraża się ona m.in. poprzez wykonywanie analiz bieżących i okresowych raportów spółek publicznych, działających na rynku regulowanym, a w przypadku wykrycia nieprawidłowości – poprzez przeprowadzanie kontroli i postępowania wyjaśniającego (z ewentualnym uwzględnieniem dalszego postępowania administracyjnego) oraz nakładanie na emitentów papierów wartościowych oraz osoby pełniące w nich funkcje zarządcze stosownych kar za naruszenie prawa.
Zasadniczym celem artykułu jest ilościowa i wartościowa analiza sankcji cywilnoprawnych nakładanych przez KNF na emitentów papierów wartościowych oraz podmioty z nimi powiązane w związku z niewypełnianiem lub nierzetelnym wypełnianiem obowiązku informacyjnego na podstawie przepisów prawa. Badania empiryczne zostały zrealizowane na podstawie danych widniejących na witrynie internetowej PAP i przekazywanych do publicznej wiadomości za pośrednictwem Elektronicznego Systemu Przekazywania Informacji (ESPI).

Słowa kluczowe: obowiązek informacyjny, Komisja Nadzoru Finansowego, spółki giełdowe
Kody klasyfikacji JEL: K20, M42, M48

1. Wprowadzenie

Rynek regulowany jest tym systemem obrotu instrumentami finansowymi, który zakłada konieczność udostępniania wszystkim inwestorom równego i powszechnego dostępu do informacji rynkowej w tym samym czasie przy kojarzeniu ofert nabycia i zbycia instrumentów finansowych. Należyte wypełnienie obowiązków informacyjnych przez spółki uczestniczące w zorganizowanym rynku kapitałowym nie powinno być jednak postrzegane tylko i wyłącznie jako wymóg stawiany emitentom papierów wartościowych przez ustawodawcę. Zasadniczym celem udostępniania informacji przez uczestników rynku giełdowego jest dążenie do wyeliminowania asymetrii informacyjnej, prowadzącej zwykle do uprzywilejowania tej części inwestorów, która z racji pełnionych funkcji dysponuje szerszą wiedzą na temat wyników finansowych osiąganych przez spółki giełdowe, planów dotyczących ich fuzji lub przejęć, czy też aktualnego poziomu popytu i podaży na dane instrumenty finansowe, bądź też która bezpośrednio uczestniczy w operacjach obrotu papierami wartościowymi na rynku kapitałowym.

Z punktu widzenia inwestora, bieżące i okresowe raporty publikowane przez emitentów papierów wartościowych przyczyniają się do stworzenia bazy informacyjnej, na podstawie której możliwe staje się dokonanie oceny ich sytuacji finansowej i perspektyw rozwojowych. Z kolei z punktu widzenia emitentów papierów wartościowych, transparentna polityka informacyjna przyczyniać się może do: wzrostu zaufania inwestorów, zmniejszenia kosztu pozyskania kapitału w drodze zwiększania płynności obrotu papierami wartościowymi[1], zmniejszenia kosztów pozyskania finansowania dłużnego (w drodze emisji obligacji), podwyższenia ratingu, zmniejszenia kosztów monitorowania rynku przez inwestorów, a w konsekwencji do sytuacji, w której kurs akcji w jak największym stopniu odzwierciedla sytuację gospodarczą i finansową emitenta[2].

[1] A. Duliniec, *Finansowanie przedsiębiorstwa*, PWE, Warszawa 2007, s. 45.

[2] M. Zaleśkiewicz, *Nowe regulacje dotyczące obowiązków informacyjnych spółek giełdowych*, Departament Nadzoru Obrotu, Urząd Komisji Nadzoru Finansowego, Warszawa 2015, s. 3.

Wypełnianie obowiązków informacyjnych charakteryzować się powinno prawdziwością, rzetelnością i kompletnością, a także odzwierciedlaniem specyfiki opisywanej sytuacji[3]. W Polsce nadzór nad prawidłowym wypełnianiem obowiązków informacyjnych przez emitentów papierów wartościowych dopuszczonych do obrotu na rynku regulowanym sprawuje Komisja Nadzoru Finansowego (KNF). W jej kompetencjach leży wykonywanie analiz bieżących i okresowych raportów spółek notowanych na Głównym Rynku GPW, a w przypadku wykrycia nieprawidłowości – przeprowadzanie kontroli i postępowania wyjaśniającego oraz nakładanie na emitentów papierów wartościowych i osoby pełniące w nich funkcje zarządcze stosownych kar za naruszenie prawa. Choć odpowiedzialność prawna, związana z obowiązkiem raportowania, może sprowadzać się do odpowiedzialności: administracyjnej, karnej oraz cywilnej, od wielu lat notuje się liczne przykłady potwierdzające nieprzestrzeganie tychże obostrzeń w praktyce[4].

Zasadniczym celem artykułu jest ilościowa i wartościowa analiza sankcji cywilnoprawnych nakładanych przez KNF na emitentów papierów wartościowych oraz podmioty z nimi powiązane w związku z niewypełnianiem lub nierzetelnym wypełnianiem obowiązku informacyjnego na podstawie przepisów Ustawy z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych i Ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi w okresie 2008–2016. Przeprowadzone badania uwzględniają zarówno analizę porównawczą w czasie, jak

[3] Patrz: Rozdział 1, § 3.1. Rozporządzenia Ministra Finansów z dnia 19 lutego 2009 r. w sprawie informacji bieżących i okresowych przekazywanych przez emitentów papierów wartościowych oraz warunków uznawania za równoważne informacji wymaganych przepisami prawa państwa niebędącego państwem członkowskim.

[4] Problem nieprzestrzegania zasad związanych z wypełnianiem obowiązku informacyjnego jest szeroko rozpatrywany na niwie zarówno krajowej, jak i zagranicznej literatury przedmiotu. Do najważniejszych pozycji poświęconych opisywanej tematyce zaliczyć należy m.in.: R. Karmel, *Outsider Trading on Confidential Information: A Breech in Search of a Duty*, „BrooklynWorks" 1998, no. 9, s. 83–133; J.M. Sheffey, *Securities Law Responsibilities of Issuers to Respond to Rumors and Other Publicity: Reexamination of a Continuing Problem*, „Notre Dame Law Review" 1982, vol. 57(5), s. 755–797; A. Fleischer, R.M. Mundheim, J.C. Murphy, *An Initial Inquiry into the Responsibility to Disclose Market Information,* „University of Pennsylvania Law Review" 1973, no. 121, s. 799–858; F.F. Coulom, *Rule 10b-5 and the Duty to Disclose Market Information: It Takes a Thief*, „St. John's Law Review" 2012, vol. 55, iss. 1, s. 93–123; A.J. VanGetson, *Real-Time Disclosure of Securities Information via the Internet: Real-Time or Not Right Now?*, „Journal of Law, Technology and Policy" 2003, vol. 2, s. 551–571; F.P. Manns Jr., *Duty to Correct: A Suggested Framework*, „Maryland Law Review" 1987, vol. 46, s. 1250–1265; K. Klimczak, *Naruszenia obowiązków informacyjnych przez spółki notowane na NewConnect*, w: *Współczesne uwarunkowania sprawozdawczości i rewizji finansowej*, red. J. Krasodomska, K. Świetla, Fundacja Uniwersytetu Ekonomicznego w Krakowie, Kraków 2015, s. 227–240.

i analizę zróżnicowania legislacyjnych podstaw wymierzania tychże kar. Badania empiryczne zostały zrealizowane na podstawie danych widniejących na witrynie internetowej Polskiej Agencji Prasowej i przekazywanych do publicznej wiadomości za pośrednictwem Elektronicznego Systemu Przekazywania Informacji (ESPI).

2. Obowiązek informacyjny spółek notowanych na regulowanym rynku w świetle obowiązującego ustawodawstwa

Do dnia 2 lipca 2016 r. rodzaj, zakres oraz formę informacji przekazywanych przez spółki giełdowe notowane na Głównym Rynku GPW w Warszawie w szczególności określały: rozporządzenie Ministra Finansów z dnia 19 lutego 2009 r. w sprawie informacji bieżących i okresowych przekazywanych przez emitentów papierów wartościowych oraz warunków uznawania za równoważne informacji wymaganych przepisami prawa państwa niebędącego państwem członkowskim (Dz.U. nr 33, poz. 259 z późn. zm)[5], ustawa z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (Dz.U. nr 184, poz. 1539 z późn. zm.)[6]

[5] Rozporządzenie regulowało obowiązki informacyjne związane z upublicznianiem raportów bieżących oraz okresowych. Definiowało ono m.in. dokładny katalog informacji, które należało publikować w formie raportów bieżących, i zakres niezbędnych informacji, sprawozdań i oświadczeń, które obowiązkowo wchodziły w skład przekazywanych raportów okresowych: kwartalnych, półrocznych oraz rocznych (jednostkowych i skonsolidowanych – dla wybranych grup emitentów papierów wartościowych).

[6] Ustawa nakładała wymóg publikowania informacji o ujawnieniu stanu posiadania. Dotyczył on każdego akcjonariusza, który: osiągnął lub przekroczył 5%, 10%, 15%, 20%, 25%, 33%, 33,33%, 50%, 75% albo 90% ogólnej liczby głosów w spółce publicznej; posiadał co najmniej 5%, 10%, 15%, 20%, 25%, 33%, 33,33%, 50%, 75% albo 90% ogólnej liczby głosów w tej spółce, a w wyniku zmniejszenia tego udziału osiągnął odpowiednio 5%, 10%, 15%, 20%, 25%, 33%, 33,33%, 50%, 75% albo 90% lub mniej ogólnej liczby głosów. Ponadto ustawa nakładała obowiązek informacyjny w związku z przekazywaniem przez emitentów papierów wartościowych wykazu akcjonariuszy uprawnionych do udziału w Walnym Zgromadzeniu, z określeniem liczby akcji i głosów z akcji przysługujących każdemu z nich (przed jego rozpoczęciem) oraz przekazywaniem wykazu akcjonariuszy posiadających co najmniej 5% liczby głosów na Walnym Zgromadzeniu, z określeniem liczby głosów przysługujących każdemu z nich z posiadanych akcji i wskazaniem ich procentowego udziału w liczbie głosów na Walnym Zgromadzeniu oraz w ogólnej liczbie głosów (po jego zakończeniu). Warto odnotować, że ustawa definiowała również termin „informacja poufna". Zgodnie z zapisami ustawy informacją poufną jest – określona w sposób precyzyjny – informacja dotycząca, bezpośrednio lub pośrednio, jednego lub kilku emitentów instrumentów finansowych, jednego lub kilku instrumentów finansowych albo nabywania lub zbywania takich instrumentów, która nie została przekazana do publicznej wiadomości, a która po takim

oraz ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U. nr 183, poz. 1538, z późn. zm.)[7]. Zawarte w nich przepisy prawne uwzględniały konieczność udostępniania właścicielom akcji oraz przyszłym inwestorom dostępu do: bieżących informacji na temat emitentów papierów wartościowych, informacji poufnych (rozumianych wg art. 154 ustawy o obrocie instrumentami finansowymi) oraz raportów okresowych. Określały one nadto katalog okoliczności, które wymagały stosownych publikacji, jak również ściśle ustalone terminy wypełniania obowiązków informacyjnych. W tym miejscu wskazać należy, że z obowiązków raportowania na gruncie prawa polskiego wywiązywać się muszą nie tylko emitenci papierów wartościowych, lecz także insiderzy rynku kapitałowego, którzy są obowiązani do informowania Komisji Nadzoru Finansowego oraz podmiotu, którego są akcjonariuszami, o wykonanych transakcjach na akcjach[8].

W dniu 3 lipca 2016 r. we wszystkich krajach członkowskich Unii Europejskiej rozpoczęło się stosowanie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku oraz uchylającego dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywę Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE (tzw. rozporządzenie Market Abuse Regulation, MAR)[9]. W Polsce nowelizacja ustaw: o obrocie instrumentami finansowymi i o ofercie publicznej, która ostatecznie dostosowała krajowe przepisy do unijnego rozporządzenia MAR, weszła w życie 6 maja 2017 r.

przekazaniu mogłaby w istotny sposób wpłynąć na cenę tych instrumentów finansowych lub na cenę powiązanych z nimi pochodnych instrumentów finansowych.

[7] Zapisy ustawy odnosiły się do obowiązków związanych z publikowaniem raportów bieżących przez emitentów spółek giełdowych i insiderów rynku giełdowego. Nakładały one konieczność publikacji informacji o transakcjach nabycia lub zbycia wyemitowanych przez nią papierów wartościowych, dokonywanych przez osoby wchodzące w skład organów zarządzających lub nadzorczych emitenta albo będące jego prokurentami i innych osób pełniących funkcje kierownicze, które posiadają stały dostęp do informacji poufnych dotyczących bezpośrednio lub pośrednio tego emitenta oraz kompetencje w zakresie podejmowania decyzji wywierających wpływ na jego rozwój i perspektywy prowadzenia działalności gospodarczej.

[8] A. Strzelczyk, *Obowiązki informacyjne spółek giełdowych – analiza komunikatów*, „Zeszyty Naukowe Wyższej Szkoły Bankowej we Wrocławiu" 2013, nr 2(34), s. 412.

[9] Rozporządzenie MAR zostało uchwalone w dniu 16 kwietnia 2014 r., a niektóre jego przepisy weszły w życie w dniu 2 lipca 2014 r., jednakże w odniesieniu do najbardziej istotnych postanowień wprowadzono dwuletnie *vacatio legis*, aby umożliwić emitentom dostosowanie się do działania w zmienionym otoczeniu regulacyjnym. M. Kozicki, *Rozporządzenie MAR (Market Abuse Regulation) i Dyrektywa MAD II (Market Abuse Directive)*, „Alert Prawny" 2016, 6, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/alerty-prawne/rozporzadzenie-mar-i-dyrektywa-mad.html, dostęp 31.10.2016.

Tabela 1. Najważniejsze zmiany związane z obowiązkiem informacyjnym spółek giełdowych, wynikające z implementacji rozporządzenia MAR w dniu 3 lipca 2016 r.

Punkt odniesienia	Zakres zmian w regulacjach prawnych
Informacja poufna	• Emitenci papierów wartościowych nie mogą stosować przewidzianego w rozporządzeniu Ministra Finansów w sprawie informacji bieżących i okresowych katalogu informacji bieżących „gospodarczych", a swoje raportowanie w tym zakresie muszą oprzeć jedynie na rozporządzeniu MAR, określającym m.in.: – obowiązek identyfikacji powstania informacji poufnej, – obowiązek niezwłocznego podania do wiadomości publicznej informacji poufnej, – obowiązek zamieszczenia informacji poufnej w systemie scentralizowanego gromadzenia informacji regulowanych OAM (w stosownych przypadkach), – obowiązek zamieszczenia i utrzymywania przez 5 lat na stronie internetowej informacji poufnej. • Upublicznienie informacji poufnej należy wykonać niezwłocznie. Oznacza to, iż odpadł drugi maksymalny, przewidziany w ustawie o ofercie publicznej, 24-godzinny termin na publikację informacji poufnych
Opóźnianie informacji poufnej	• Zmiana przesłanek dopuszczalności opóźnienia publikacji informacji poufnej. Rozporządzenie MAR dopuszcza opóźnienie w przypadku: – ryzyka naruszenia prawnie uzasadnionego interesu emitenta; – gdy opóźnienie prawdopodobnie nie wprowadzi w błąd opinii publicznej; – gdy emitent jest w stanie zapewnić poufności informacji (gdy poufność nie może być zagwarantowania – obowiązek publikacji); dotychczas stosowane przepisy umożliwiały opóźnienie w publikacji informacji poufnej w sytuacji, gdy ujawnienie informacji mogłoby naruszyć słuszny interes emitenta i tylko w odniesieniu do określonego czasu. • Brak wskazania przypadków opóźnienia informacji poufnych. • Brak obowiązku uprzedniego poinformowania KNF
Transakcje insiderów	• Zmiana zakresu podmiotowego insiderów zobligowanych do upubliczniania informacji o przeprowadzanych transakcjach. Rozporządzenie MAR zalicza do nich: osoby pełniące obowiązki zarządcze oraz osoby blisko związane z osobami pełniącymi obowiązki zarządcze. Ustawodawstwo obowiązujące do dnia 3 lipca 2016 r. do grona insiderów, których dotyczył obowiązek informacyjny, zaliczało: członków zarządu i rady nadzorczej, prokurentów, jak również inne osoby pełniące w strukturze emitenta funkcje kierownicze, które posiadają stały dostęp do informacji poufnych oraz kompetencje w zakresie podejmowania decyzji, wywierających wpływ na jego rozwój i perspektywy prowadzenia działalności gospodarczej
Okresy zamknięte	• Emitent może zezwolić na dokonywanie transakcji w trakcie okresu zamkniętego: – na podstawie indywidualnych przypadków z powodu istnienia wyjątkowych okoliczności, takich jak poważne trudności finansowe; – z powodu cech danej transakcji, dokonywanej w ramach programu akcji pracowniczych, programów oszczędnościowych, kwalifikacji lub uprawnień do akcji, lub też transakcji, w których korzyść związana z danym papierem wartościowym nie ulega zmianie, lub cech transakcji z nimi związanych
Nadzór KNF	• Pod nadzór Komisji Nadzoru Finansowego trafią dodatkowo wszystkie spółki notowane na NewConnect

Źródło: opracowanie własne na podstawie: M. Zaleśkiewicz, *Nowe regulacje dotyczące obowiązków informacyjnych spółek giełdowych*, Departament Nadzoru Obrotu, Urząd Komisji Nadzoru Finansowego, Warszawa 2015, s. 19–30.

Z perspektywy spółek giełdowych, rozporządzenie MAR reguluje obowiązki związane z przekazywaniem informacji poufnych oraz procedurę opóźniania publikacji tych informacji, jak również obowiązki dotyczące prowadzenia wykazów osób mających dostęp do informacji poufnych. Zakres raportowania jest przy tym jednakowy zarówno dla emitentów papierów wartościowych dopuszczonych do obrotu na rynku regulowanym, jak i emitentów papierów wartościowych wprowadzonych do alternatywnego systemu obrotu. W tabeli 1 przedstawiono najważniejsze zmiany związane z obowiązkiem informacyjnym, wynikające z wdrożenia zapisów rozporządzenia MAR w Polsce.

3. Odpowiedzialność prawna grożąca emitentom papierów wartościowych oraz podmiotom powiązanym z tytułu nienależytego wypełniania obowiązków informacyjnych

Jednym z organów czuwających nad bezpieczeństwem uczestników rynku giełdowego jest Komisja Nadzoru Finansowego. Jej rola nadzorcza nad rynkiem finansowym wiąże się z zapewnieniem prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnieniem ochrony interesów uczestników tego rynku[10]. Działalność KNF w znacznej mierze ukierunkowana jest na przeciwdziałanie przestępstwom przeciwko rynkowi kapitałowemu. W literaturze przedmiotu do takich zalicza się przede wszystkim[11]:

- wykorzystywanie informacji wewnętrznych (ang. *insider trading*), polegające na użyciu posiadanej informacji poufnej w celu osiągnięcia korzyści finansowej, na skutek zakupu lub sprzedaży walorów spółki, której ta informacja dotyczy;
- manipulację rynkiem (ang. *manpiluation*), będącą czynem przestępczym, polegającym na „stworzeniu iluzji" innym uczestnikom rynku o dalszych możliwościach

[10] Szerzej: http://www.knf.gov.pl/o_nas/komisja/index.html.

[11] M. Dusza, *Rynek kapitałowy w Polsce – narodziny, pierwsze dziesięciolecie, perspektywy*, Biblioteka Menedżera i Bankowca, Warszawa 1999, za: B. Karaban, *Zjawisko asymetrii informacyjnej i niewiedzy uczestników rynku na przykładzie rynku kapitałowego w Polsce*, http://www.kapital.edu.pl/pliki/wyroznione_prace/B_ Karaban-Asymetria_informacyjna_i_niewiedza_uczestnikow_rynku_KARABAN.pdf, dostęp 31.10.2016.

zmian kursu w celu skłonienia ich do podjęcia decyzji inwestycyjnych korzystnych dla manipulującego;
- uprzedzanie operacji (ang. *front running*), będące techniką polegającą na dokonaniu przez maklera najpierw jego operacji w określonych papierach wartościowych, a dopiero później operacji klienta, która – jak sądzi – ze względu na swoją wielkość spowoduje zmianę notowań rynkowych tego papieru;
- przelewanie (ang. *churning*, *overtrade*, *twisting*), polegające na dokonywaniu zbędnych operacji, nieuzasadnionych warunkami rynkowymi, w celu uzyskania prowizji należnej z tytułu obrotu instrumentami finansowymi.

Obowiązujące na podstawie ustawy z dnia 29 lipca 2005 r. o ofercie publicznej oraz ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi prawo przewiduje zróżnicowane sankcje administracyjnoprawne względem emitentów papierów wartościowych. Mogą one obejmować: kary pieniężne, zawieszenie obrotu lub wykluczenie z obrotu instrumentów finansowych emitenta (sankcje względem emitentów) oraz kary pieniężne (po uprzednim nałożeniu kary na emitenta za rażące naruszenie prawa – sankcje względem członków zarządu emitenta). Ponadto dopuszczona jest możliwość ponoszenia odpowiedzialności prawnej w formie sankcji karnej (zwłaszcza gdy w odniesieniu do istotnych informacji podawane były informacje nieprawdziwe lub informacje prawdziwe były zatajane) oraz odpowiedzialności cywilnej (dotyczącej konieczności naprawienia akcjonariuszom wyrządzonej szkody z tytułu nieprawidłowego wypełniania obowiązków informacyjnych)[12]. Implementowane w dniu 3 lipca 2016 r. rozwiązania prawne w związku rozporządzeniem MAR nie definiują wprost wysokości pieniężnych kar administracyjnych nakładanych z tytułu naruszeń obowiązków informacyjnych. Określają one jednak górne granice sankcji, które są znacząco wyższe niż obowiązujące w prawie polskim do dnia wdrożenia omawianego rozporządzenia (tabela 2). Zauważyć jednak trzeba, że brak pełnego dostosowania przepisów krajowych do rozporządzenia MAR powoduje pewne trudności w zakresie interpretacji niektórych przepisów.

[12] Zob. art. 96 pkt 1 oraz art. 101 pkt 1 Ustawy z dnia 29 lipca 2005 r. o ofercie publicznej; art. 181 pkt 1, art. 183 pkt 1 oraz art. 183 pkt 2 Ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.

Tabela 2. Maksymalna wysokość kar za niewywiązywanie lub nienależyte wywiązywanie się z obowiązków informacyjnych, określona w rozporządzeniu MAR

Charakter naruszonego przepisu	Grożąca sankcja prawna	
	osoby fizyczne	osoby prawne
Obowiązek podania informacji poufnej do publicznej wiadomości	1 mln euro	2,5 mln euro lub 2% obrotów
Obowiązek dotyczący list osób mających dostęp do informacji poufnych	500 tys. euro	1 mln euro
Obowiązek dotyczący transakcji osób pełniących obowiązki zarządcze	500 tys. euro	1 mln euro
Dokonywanie transakcji w trakcie okresu zamkniętego	500 tys. euro	1 mln euro

Źródło: jak pod tab. 1, s. 28.

4. Sankcje nakładane przez KNF w związku z naruszaniem przepisów Ustawy o ofercie publicznej

Z wyników przeprowadzonych badań empirycznych wynika, że w okresie 2008–2016[13] Komisja Nadzoru Finansowego nałożyła łącznie 207 kar w związku z niewypełnianiem lub nienależytym wypełnianiem obowiązku informacyjnego na podstawie przepisów Ustawy o ofercie publicznej. Sumaryczna wartość omawianych kar wyniosła 42 374 tys. zł (tabela 3), przy czym 37 740 tys. zł stanowiły kary wymierzone względem osób prawnych, zaś 4594 tys. zł to kary nałożone na osoby fizyczne.

W generalnym ujęciu zauważyć należy, że w horyzoncie 2008–2016 KNF za naruszanie przepisów ustawy o ofercie publicznej stosowała zróżnicowane co do wartości kary finansowe. Świadczyć o tym może statystyczne ujęcie rozkładu wartości tychże kar, sporządzone z perspektywy sankcji nakładanych zarówno na osoby fizyczne, jak i na osoby prawne (tabela 4).

[13] Stan na dzień 31.10.2016.

Tabela 3. Ilościowa oraz wartościowa charakterystyka kar finansowych nakładanych przez KNF z związku z niewywiązywaniem lub nienależytym wywiązywaniem się z obowiązków informacyjnych określonych w ustawie o ofercie publicznej w okresie 2008–2016

Lata	Podstawa wymierzenia kary finansowej przez KNF – osoby prawne i osoby fizyczne							
	Naruszenie art. 10, 56 lub 57 ustawy o ofercie publicznej – osoby prawne		Naruszenie art. 10, 56 lub 57 ustawy o ofercie publicznej – osoby fizyczne		Naruszenie art. 69, 70, 72–74 lub 76 ustawy o ofercie publicznej – osoby prawne		Naruszenie art. 69, 70, 72–74 lub 76 ustawy o ofercie publicznej – osoby fizyczne	
	Wartość nałożonych kar (w zł)	Liczba kar	Wartość nałożonych kar (w zł)	Liczba kar	Wartość nałożonych kar (w zł)	Liczba kar	Wartość nałożonych kar (w zł)	Liczba kar
2008	520 000,00	8	94 000,00	3	375 000,00	5	390 000,00	10
2009	1 160 000,00	13	200 000,00	2	240 000,00	7	622 000,00	4
2010	2 470 000,00	17	80 000,00	1	60 000,00	2	410 000,00	4
2011	1 370 000,00	11	495 000,00	7	1 880 000,00	8	502 000,00	7
2012	1 100 000,00	10	140 000,00	4	1 260 000,00	7	70 000,00	2
2013	3 375 000,00	13	145 000,00	3	11 730 000,00	9	331 000,00	3
2014	3 350 000,00	8	165 000,00	3	80 000,00	3	70 000,00	1
2015	1 340 000,00	7	390 000,00	4	2 060 000,00	4	410 000,00	2
2016	5 290 000,00	12	94 000,00	1	120 000,00	2	390 000,00	0
Razem	19 975 000,00	99	1 789 000,00	28	17 805 000,00	47	2 805 000,00	33

Źródło: opracowanie własne na podstawie: *Wykaz kar nałożonych przez KNF – wg naruszeń*, http://bip.knf.gov.pl/?l=/Komisja/050_Kary/kary.html, dostęp 31.10.2016.

Tabela 4. Statystyka rozkładu wartości kar finansowych nakładanych przez KNF z związku z niewywiązywaniem lub nienależytym wywiązywaniem się z obowiązków informacyjnych określonych w ustawie o ofercie publicznej w okresie 2008–2016

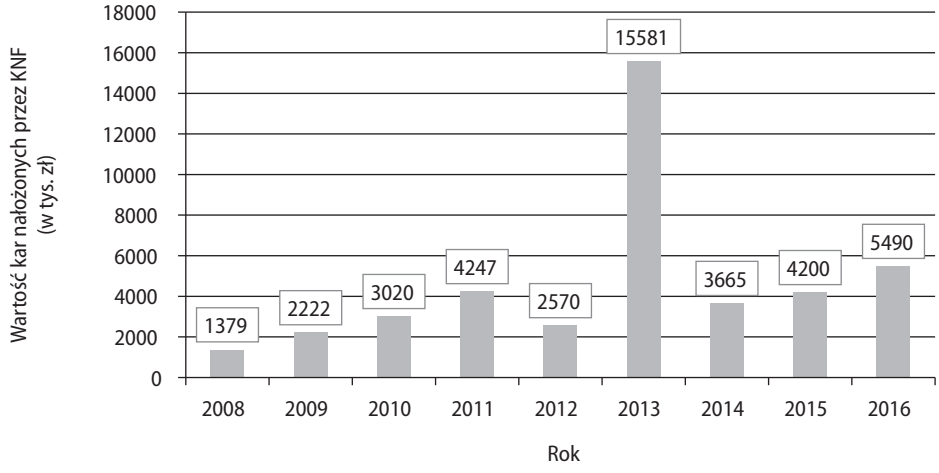
Miara statystyczna	Wartość (w zł)	
	osoby prawne	osoby fizyczne
Średnia arytmetyczna	258 767,12	76 816,67
Mediana	85 000,00	67 500,00
Minimum	10 000,00	1 000,00
Maksimum	5 720 000,00	500 000,00

Źródło: jak pod tab. 3.

Zwrócić należy uwagę na fakt, że najwyższa łączna wartość kar finansowych nałożonych przez KNF za naruszenie przepisów ustawy o ofercie publicznej przypadła na 2013 r. (rysunek 1). Wtedy też ustanowione zostały dwie najwyższe sankcje finansowe w historii polskiego rynku regulowanego za niewypełnianie lub nienależyte wypełnianie obowiązku informacyjnego. Sankcje te tyczyły się następujących podmiotów:

– Platinum Prestige Capital SA – kara w wysokości 5630 tys. zł za trzydziestojednokrotne naruszenie obowiązków informacyjnych, związanych ze znacznymi pakietami akcji spółki PSW Capital SA w okresie październik 2010 r. – grudzień 2012 r.,
– Domu Inwestycyjnego Platinum Capital SA – kara w wysokości 5720 tys. zł za czterdziestokrotne naruszenie obowiązków informacyjnych związanych ze znacznymi pakietami akcji spółki publicznej PSW Capital SA w okresie czerwiec 2010 r. – grudzień 2012 r.

Rysunek 1. Sumaryczna wartość kar finansowych nakładanych przez KNF z związku z niewywiązywaniem lub nienależytym wywiązywaniem się z obowiązków informacyjnych określonych w ustawie o ofercie publicznej w poszczególnych latach okresu 2008–2016

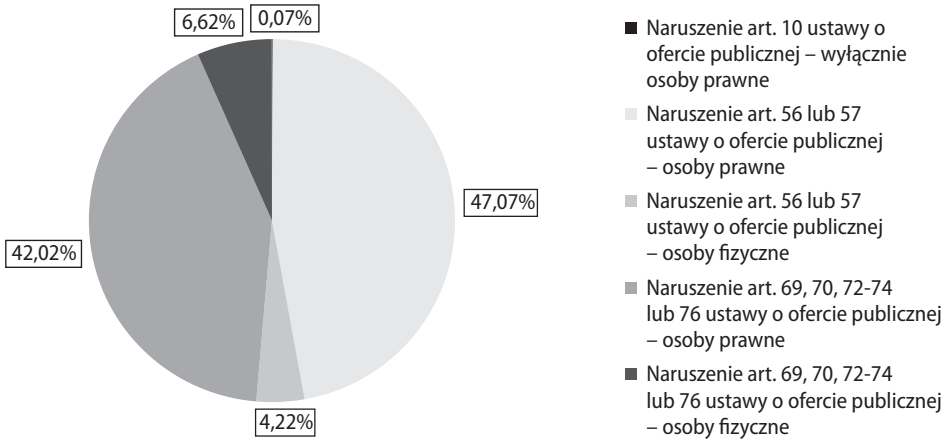


Źródło: opracowanie własne na podstawie: *Wykaz kar nałożonych przez KNF – wg naruszeń*, http://bip.knf.gov.pl/?l=/Komisja/050_Kary/kary.html, dostęp 31.10.2016.

Biorąc pod uwagę podstawę prawną wymierzanych przez KNF kar finansowych, zauważyć należy dominację – zarówno pod względem ilościowym, jak

i wartościowym – sankcji nakładanych na emitentów papierów wartościowych i podmioty z nimi powiązane w związku z naruszaniem przepisów dotyczących konieczności równoczesnego przekazywania do: KNF, spółki prowadzącej rynek regulowany oraz publicznej wiadomości informacji poufnych, bieżących bądź okresowych (naruszenie art. 56 ustawy) lub też w związku z nieuzasadnionym prawnie opóźnieniem wykonania obowiązków informacyjnych przez emitenta (naruszenie art. 57 ustawy). Sankcje te stanowiły ponad 47% wartości kar finansowych ogółem, nałożonych przez KNF w horyzoncie 2008–2016 w związku z naruszeniem przepisów ustawy o ofercie publicznej (rysunek 2). Warto jednocześnie dodać, iż ponad 42% wartości wszystkich kar finansowych wymierzonych względem spółek giełdowych i podmiotów z nimi powiązanych stanowiły sankcje za nieprzestrzeganie obowiązku informacyjnego związanego z: ujawnieniem stanu posiadania (art. 69 ustawy), obowiązkiem wykazania akcjonariuszy uprawnionych do udziału w walnym zgromadzeniu i akcjonariuszy posiadających co najmniej 5% liczby głosów na tym zgromadzeniu (art. 70 ustawy) oraz ogłoszeniem wezwania do zapisywania się na sprzedaż lub zamianę akcji danej spółki (art. 72–74, 76 ustawy).

Rysunek 2. Struktura kar finansowych nakładanych przez KNF z związku z niewywiązywaniem lub nienależytym wywiązywaniem się z obowiązków informacyjnych określonych w ustawie o ofercie publicznej w okresie 2008–2016 – według charakteru naruszeń



Źródło: jak pod rys. 1.

Dla porządku należy dodać, że poza karami finansowymi ustawodawstwo polskie przyznało KNF dodatkowe narzędzia sankcjonowania emitentów papierów wartościowych, członków ich organów zarządzających, prokurentów emitenta oraz pozostałe osoby pełniące funkcje kierownicze w strukturze organizacyjnej emitenta za niewypełnianie lub nienależyte wypełnianie obowiązku raportowania. Przykładowo, w 2010 r. KNF (poza karą finansową w wysokości 50 tys. zł) ukarała spółkę Techmex SA dodatkowym wykluczeniem papierów wartościowych z obrotu na okres 12 miesięcy[14]. Był to jednak ten rodzaj sankcji, który spotkał się z jednorazowym zastosowaniem ze strony KNF w przyjętym okresie odniesienia.

5. Sankcje nakładane przez KNF w związku z naruszaniem przepisów ustawy o obrocie instrumentami finansowymi

Analiza przeprowadzonych badań empirycznych wykazała, że w okresie 2008–2016 KNF, w związku z łamaniem przepisów dotyczących obowiązku informacyjnego na podstawie artykułów ustawy o obrocie instrumentami finansowymi, wymierzyła łączne kary finansowe opiewające na kwotę 2671 tys. zł (tabele 5 i 6). Z punktu widzenia struktury tychże kar, około 75,3% ich wartości (tj. 2011 tys. zł) obejmowało sankcje nałożone na osoby fizyczne, pozostałą zaś część (tj. 660 tys. zł) stanowiły kary finansowe względem osób prawnych. Warto jednocześnie zwrócić uwagę na fakt, że osoby fizyczne były zdecydowanie częściej obarczane wspomnianymi sankcjami (31 przypadków kar) niż osoby prawne (5 przypadków kar).

[14] Spółka Techmex SA została ukarana za nieprzekazanie do publicznej wiadomości informacji poufnej o złożeniu przez syndyka masy upadłościowej zawiadomienia o uzasadnionym podejrzeniu popełnienia przestępstwa i powiadomieniu Krajowej Izby Biegłych Rewidentów w związku z brakiem prawdziwości i rzetelności danych finansowych zawartych w sprawozdaniach finansowych opublikowanych przez spółkę przed ogłoszeniem jej upadłości, polegającym w szczególności na kilkukrotnym zawyżeniu wyniku finansowego wskazanego w sprawozdaniu finansowym sporządzonym przez zarząd spółki na dzień 30 września 2009 r.

Tabela 5. Ilościowa oraz wartościowa charakterystyka kar finansowych nakładanych na osoby prawne przez KNF z związku z niewywiązywaniem lub nienależytym wywiązywaniem się z obowiązków informacyjnych określonych w ustawie o obrocie instrumentami finansowymi w okresie 2008–2016

Rok	Podstawa wymierzenia kary finansowej przez KNF – osoby prawne							
	Naruszenie art. 24 ustawy o obrocie instrumentami finansowymi		Naruszenie art. 107 ustawy o obrocie instrumentami finansowymi		Naruszenie art. 160 ustawy o obrocie instrumentami finansowymi		Naruszenie art. 167 ustawy o obrocie instrumentami finansowymi	
	Wartość nałożonych kar (w zł)	Liczba kar	Wartość nałożonych kar (w zł)	Liczba kar	Wartość nałożonych kar (w zł)	Liczba kar	Wartość nałożonych kar (w zł)	Liczba kar
2008	–	–	–	–	–	–	–	–
2009	–	–	–	–	–	–	–	–
2010	–	–	–	–	–	–	–	–
2011	–	–	–	–	10 000,00	1	–	–
2012	–	–	–	–	–	–	150 000,00	1
2013	–	–	–	–	–	–	–	–
2014	–	–	70 000,00	1	–	–	–	–
2015	–	–	–	–	400 000,00	1	–	–
2016	30 000,00	1	–	–	–	–	–	-
Razem	30 000,00	1	70 000,00	1	410 000,00	2	150 000,00	1

Źródło: jak pod tab. 3.

Należy również zauważyć, że ze statystycznego punktu widzenia wartość kar nakładanych przez KNF w związku z naruszaniem obowiązku raportowania na podstawie ustawy o obrocie instrumentami finansowymi była relatywnie niższa niż wartość kar wymierzanych za niewywiązywanie lub nienależyte wywiązywanie się z obowiązków informacyjnych określonych w ustawie o ofercie publicznej (tabela 7). Na podstawie średnich 9-letnich wartości sankcji finansowych nakładanych na osoby prawne w związku z nieprzestrzeganiem artykułów ustawy o obrocie można orzec, że stosowane względem wskazanych podmiotów kary były dwukrotnie niższe od przeciętnych kar nakładanych za naruszenie obowiązków informacyjnych wynikających z ustawy o ofercie publicznej. Z punktu widzenia osób fizycznych różnice te nie są już tak widoczne.

Tabela 6. Ilościowa oraz wartościowa charakterystyka kar finansowych nakładanych na osoby fizyczne przez KNF z związku z niewywiązywaniem lub nienależytym wywiązywaniem się z obowiązków informacyjnych określonych w ustawie o obrocie instrumentami finansowymi w okresie 2008–2016

Rok	Podstawa wymierzenia kary finansowej przez KNF – osoby fizyczne							
	Naruszenie art. 39 ustawy o obrocie instrumentami finansowymi		Naruszenie art. 159 ustawy o obrocie instrumentami finansowymi		Naruszenie art. 160 ustawy o obrocie instrumentami finansowymi		Naruszenie art. 106 ust. 1 ustawy o obrocie instrumentami finansowymi	
	Wartość nałożonych kar (w zł)	Liczba kar	Wartość nałożonych kar (w zł)	Liczba kar	Wartość nałożonych kar (w zł)	Liczba kar	Wartość nałożonych kar (w zł)	Liczba kar
2008	–	–	136 000,00	6	24 000,00	9	30 000,00	1
2009	300 000,00	2	1 000,00	1	–	–	–	–
2010	100 000,00	1	–	–	–	–	–	–
2011	300 000,00	2	–	–	–	–	–	–
2012	–	–	110 000,00	2	–	–	–	–
2013	150 000,00	1	–	–	–	–	–	–
2014	–	–	–	–	–	–	–	–
2015	560 000,00	4	200 000,00	1	–	–	–	–
2016	–	–	100 000,00	1	–	–	–	–
Razem	1 410 000,00	10	547 000,00	11	24 000,00	9	30 000,00	1

Źródło: jak pod tab. 3.

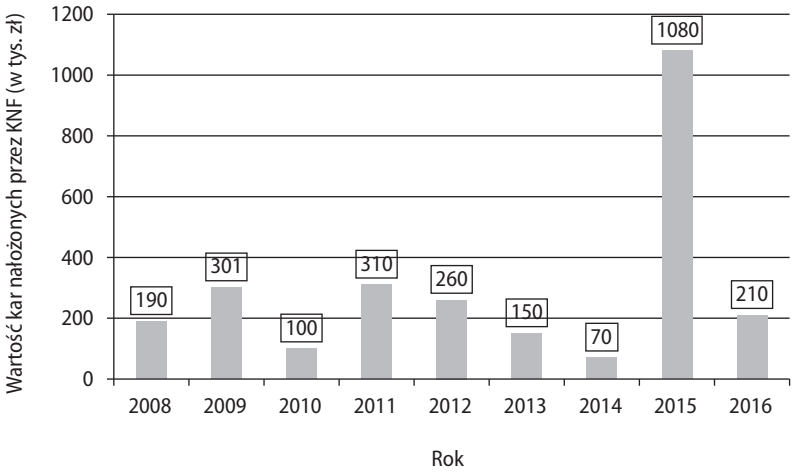
Tabela 7. Statystyka rozkładu wartości kar finansowych nakładanych przez KNF z związku z niewywiązywaniem lub nienależytym wywiązywaniem się z obowiązków informacyjnych określonych w ustawie o obrocie instrumentami finansowymi w okresie 2008–2016

Miara statystyczna	Wartość (w zł)	
	Osoby prawne	Osoby fizyczne
Średnia arytmetyczna	127 500,00	64 870,97
Mediana	50 000,00	20 000,00
Minimum	10 000,00	1 000,00
Maksimum	400 000,00	200 000,00

Źródło: jak pod tab. 3.

Przeciętna wartość kar finansowych nakładanych przez KNF wyraźnie różnicowała się z perspektywy poszczególnych lat rozpatrywanego okresu odniesienia (rysunek 3). Była ona najwyższa w 2015 roku, kiedy to osiągnęła pułap 1080 tys. zł, zaś najniższa w 2014 roku (70 tys. zł).

Rysunek 3. Sumaryczna wartość kar finansowych nakładanych przez KNF z związku z niewywiązywaniem lub nienależytym wywiązywaniem się z obowiązków informacyjnych określonych w ustawie o obrocie instrumentami finansowymi w poszczególnych latach okresu 2008–2016

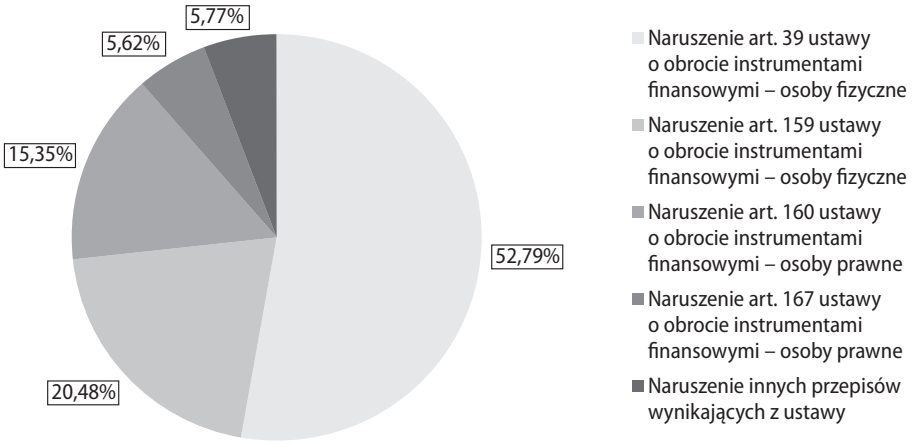


Źródło: jak pod rys. 1.

Nawiązując do prawnych podstaw nakładanych kar finansowych (w odniesieniu do naruszeń poszczególnych artykułów ustawy o obrocie instrumentami finansowymi) można orzec, że z wartościowego punktu widzenia emitenci papierów wartościowych oraz podmioty z nimi powiązane w rozpatrywanym horyzoncie badawczym byli najdotkliwiej sankcjonowani za manipulacje instrumentami finansowymi (art. 39 ustawy), w formie rozpowszechniania nierzetelnych informacji dotyczących poszczególnych podmiotów giełdowych. Kary te stanowiły ponad 52% ogółu sankcji finansowych nałożonych przez KNF za naruszenie przepisów dotyczących obowiązków informacyjnych opisanych w ustawie o obrocie instrumentami finansowymi (rysunek 4). Około 20% łącznej wartości wymierzonych kar dotyczyło złamania zakazu dokonywania transakcji instrumentami finansowymi w okresach zamkniętych (art. 159 ustawy), co zgodnie ze stanowiskiem KNF mogło prowadzić do osiągnięcia przewagi informacyjnej przez osoby pełniące funkcje publiczne.

Natomiast niewiele ponad 15% wartości omawianych sankcji wiązało się z karami za nieprzekazanie w ustawowym terminie informacji o dokonanych transakcjach akcjami spółki (art. 160 ustawy).

Rysunek 4. Struktura kar finansowych nakładanych przez KNF z związku z niewywiązywaniem lub nienależytym wywiązywaniem się z obowiązków informacyjnych określonych w ustawie o obrocie instrumentami finansowymi w okresie 2008–2016 – według naruszeń



Źródło: jak pod rys. 1.

Należy zaznaczyć, że na podstawie art. 130 ustawy o obrocie instrumentami finansowymi KNF może skreślić maklera lub doradcę z listy albo zawiesić jego uprawnienia do wykonywania zawodu na okres od 3 miesięcy do 2 lat na skutek naruszenia w związku z wykonywaniem zawodu: przepisów prawa lub regulaminów i innych przepisów wewnętrznych, do których przestrzegania makler lub doradca jest zobowiązany, zasad uczciwego obrotu lub też interesów klientów. W odniesieniu do zarzutów nierzetelnego wypełniania obowiązku informacyjnego w horyzoncie 2008–2016, KNF nałożyła na maklerów i doradców giełdowych dziesięć tego typu sankcji. Zostały one bliżej scharakteryzowane w tabeli 8.

Tabela 8. Sankcje nakładane przez KNF z związku z naruszeniem art. 130 ustawy o obrocie instrumentami finansowymi w okresie 2008–2016

Zastosowana sankcja	Charakter przewinienia	Liczba przypadków
Zawieszenie na okres 12 miesięcy uprawnień maklera papierów wartościowych	Ujawnienie tajemnicy poufnej o planowanej realizacji zlecenia na rzecz klienta	3
	Ujawnienie osobom nieuprawnionym informacji stanowiących tajemnicę zawodową, a dotyczących deklaracji nabycia akcji spółki w ofercie publicznej	1
	Wykorzystanie informacji poufnej dotyczącej planowanych wyników finansowych przed ich opublikowaniem	1
Skreślenie z listy doradców inwestycyjnych	Wykorzystanie informacji poufnej dotyczącej planowanych wyników finansowych przed ich opublikowaniem	3
Odebranie uprawnień do wykonywania zawodu maklera papierów wartościowych	Przekazanie klientowi informacji poufnej i wykorzystanie informacji poufnej poprzez złożenie stosownych dyspozycji na rachunku klienta bez umocowania	1
	Wykorzystanie informacji poufnych o zleceniach	1

Źródło: jak pod tab. 3.

6. Podsumowanie

W okresie od 1 stycznia 2008 r. do 31 października 2016 r. za pośrednictwem Elektronicznego Systemu Przekazywania Informacji (ESPI) spółki giełdowe notowane na Głównym Rynku GPW w Warszawie opublikowały łącznie 246 051 raportów okresowych i bieżących[15], niosących bezcenne z punktu widzenia inwestorów giełdowych informacje, umożliwiające bieżącą weryfikację podejmowanych decyzji przez zarząd tychże spółek oraz ocenę wytyczanych kierunków ich działalności.

W rozpatrywanym horyzoncie badawczym Komisja Nadzoru Finansowego niejednokrotnie spotkała się z naruszaniem przepisów dotyczących obligatoryjności przekazywania do publicznej wiadomości informacji poufnych, bieżących bądź okresowych, z nieuzasadnionym prawnie opóźnieniem wykonania obowiązków informacyjnych przez emitentów papierów wartościowych czy też z wykorzystywaniem informacji poufnych dla własnych lub cudzych potrzeb w sposób niezgodny z obowiązującym prawem i jednocześnie szkodliwy dla innych uczestników rynku

[15] Opracowanie własne na podstawie danych pochodzących z witryny internetowej Serwisu Ekonomicznego Polskiej Agencji Prasowej, http://biznes.pap.pl/pl/reports/espi, dostęp 31.10.2016.

giełdowego. Dla zapewnienia transparentności obrotu papierami wartościowymi na rynku regulowanym, a jednocześnie w celu minimalizacji negatywnych praktyk w zakresie wywiązywania się z obowiązków raportowania określonych w ustawach: o ofercie publicznej oraz o obrocie instrumentami finansowymi, w okresie 2008–2016 KNF nałożyła łącznie 243 kary finansowe o sumarycznej wartości 45 045 tys. zł. Dodatkowo ukarała ona jednego emitenta papierów wartościowych wykluczeniem jego akcji z obrotu na okres 12 miesięcy, zaś w stosunku do nieuczciwych maklerów oraz doradców giełdowych wystosowała dziesięć sankcji, polegających na zawieszeniu lub odebraniu uprawnień do wykonywania zawodu maklera papierów wartościowych albo też na skreśleniu z listy doradców inwestycyjnych.

Należy jednocześnie pamiętać, że rozwiązania prawne związane z zaimplementowanym w lipcu 2016 r. rozporządzeniem MAR zdecydowanie podwyższają górne granice potencjalnych sankcji, które KNF może wystosować względem osób fizycznych i prawnych za niewywiązywanie lub nienależyte wywiązywanie się z obowiązku informacyjnego. Wydaje się, że może to być skuteczna recepta na przeciwdziałanie przedstawionym w artykule nieprawidłowościom w funkcjonowaniu rynku giełdowego w Polsce.

Bibliografia

1. Coulom F.F., *Rule 10b-5 and the Duty to Disclose Market Information: It Takes a Thief*, „St. John's Law Review" 2012, vol. 55, iss. 1.
2. Duliniec A., *Finansowanie przedsiębiorstwa*, PWE, Warszawa 2007.
3. Dusza M., *Rynek kapitałowy w Polsce – narodziny, pierwsze dziesięciolecie, perspektywy*, Biblioteka Menedżera i Bankowca, Warszawa 1999.
4. Dyrektywa Parlamentu Europejskiego i Rady 2013/50/UE z dnia 22 października 2013 r.
5. Fleischer A., Mundheim R.M., Murphy J.C., *An Initial Inquiry into the Responsibility to Disclose Market Information*, „University of Pennsylvania Law Review" 1973, vol. 121.
6. Karaban B., *Zjawisko asymetrii informacyjnej i niewiedzy uczestników rynku na przykładzie rynku kapitałowego w Polsce*, http://www.kapital.edu.pl/pliki/wyroznione_prace/B_Karaban_Asymetria_informacyjna_i_niewiedza_uczestnikow_rynku_KARABAN.pdf
7. Karmel R., *Outsider Trading on Confidential Information: A Breech in Search of a Duty*, „BrooklynWorks" 1998, no. 9.

8. Klimczak K., *Naruszenia obowiązków informacyjnych przez spółki notowane na NewConnect*, *Współczesne uwarunkowania sprawozdawczości i rewizji finansowej*, red. J. Krasodomska, K. Świetla, Fundacja Uniwersytetu Ekonomicznego w Krakowie, Kraków 2015.
9. Kozicki M., *Rozporządzenie MAR (Market Abuse Regulation) i Dyrektywa MAD II (Market Abuse Directive)*, „Alert Prawny" 2016, 6, https://www².deloitte.com/pl/pl/pages/doradztwo-prawne/articles/alerty-prawne/rozporzadzenie-mar-i-dyrektywa-mad.html
10. Manns F.P. Jr., *Duty to Correct: A Suggested Framework*, „Maryland. Law Review" 1987, vol. 46.
11. Rozporządzenie Ministra Finansów z dnia 19 lutego 2009 r. w sprawie informacji bieżących i okresowych przekazywanych przez emitentów papierów wartościowych oraz warunków uznawania za równoważne informacji wymaganych przepisami prawa państwa niebędącego państwem członkowskim (Dz.U. nr 33, poz. 259).
12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku oraz uchylającego dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywę Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE.
13. Serwis Ekonomiczny Polskiej Agencji Prasowej, http://biznes.pap.pl/pl/reports/espi
14. Sheffey J.M., *Securities Law Responsibilities of Issuers to Respond to Rumors and Other Publicity: Reexamination of a Continuing Problem*, „Notre Dame Law Review" 1982, vol. 57(5).
15. Strzelczyk A., *Obowiązki informacyjne spółek giełdowych – analiza komunikatów,* „Zeszyty Naukowe Wyższej Szkoły Bankowej we Wrocławiu" 2013, nr 2(34).
16. Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U. nr 183, poz. 1538, z późn. zm.).
17. Ustawa z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (Dz.U. nr 184, poz. 1539 z późn. zm.).
18. VanGetson A.J., *Real-Time Disclosure of Securities Information via the Internet: Real-Time or Not Right Now?*, „Journal of Law, Technology and Policy" 2003, vol. 2.
19. *Wykaz kar nałożonych przez KNF – wg naruszeń*, http://bip.knf.gov.pl/?l=/Komisja/050_Kary/kary.html
20. Zaleśkiewicz M., *Nowe regulacje dotyczące obowiązków informacyjnych spółek giełdowych*, Departament Nadzoru Obrotu, Urząd Komisji Nadzoru Finansowego, Warszawa 2015.

The Contravention of Information Duty by Issuers of Securities in view of Financial Supervision Authority Sanctions

Summary

One of the competences of the Financial Supervision Authority (KNF) is the concern for the management transparency of companies whose shares are traded on the WSE Main Market. It is reflected for example through current analyses and periodic reports of public companies operating on the regulated market; and if irregularities are found by an audit and investigation procedure (with a possible further administrative procedure) and through the imposition of respective penalties on securities issuers and their managers.

The major aim of the article is a quantitative and evaluative analysis of civil law sanctions imposed by KNF on securities issuers and related entities with regard to not following or negligent following the information duty on the basis of legal regulations. The empirical research was based on the PAP website data published through the Electronic Transfer System (ESPI).

Keywords: information duty, Financial Supervision Authority, public companies