„Zeszyty Teoretyczne Rachunkowości”
tom 97 (153), 2018, s. 115–138

Stowarzyszenie Księgowych
w Polsce

Zarządzanie bezpieczeństwem zasobów informatycznych rachunkowości w polskich jednostkach – wyniki badań

ELŻBIETA IZABELA SZCZEPANKIEWICZ *

Streszczenie

Współczesne funkcjonowanie jednostek w cyberprzestrzeni pokazuje, że IT, pozwalając na nieograniczone możliwości prowadzenia biznesu i rozwoju organizacyjnego, wnosi większą liczbę wewnętrznych i zewnętrznych zagrożeń w obszarze zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości. Celem artykułu jest diagnoza aktualnego poziomu zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości w polskich jednostkach gospodarczych. W artykule przyjęto dwie hipotezy badawcze. Pierwsza stanowi, że poziom zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości w różnych grupach jednostek może się znacznie różnić, pomimo że wszystkie jednostki powinny w takim sam sposób stosować się do wymogów ustawy o rachunkowości w przedmiotowym zakresie badania. Ujawnione różnice mogą wynikać z wpływu dodatkowych regulacji sektorowych. Druga zaś, że w sektorze firm prywatnych tylko biura rachunkowe i firmy audytorskie bardziej restrykcyjnie niż inne małe i średnie firmy przestrzegają przepisów dotyczących zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości, co wiąże się z poczuciem odpowiedzialności wobec klientów. W artykule określono podstawowe uwarunkowania funkcjonowania rachunkowości jednostek w trzech wymiarach cyberprzestrzeni. Następnie zaprezentowano wyniki badań empirycznych na temat zapewnienia bezpieczeństwa informatycznego w jednostkach gospodarczych w kontekście funkcjonowania systemu kontroli wewnętrznej w obszarze rachunkowości i wypełnienia wymogów ustawy o rachunkowości. Wyniki badań pokazują, w jaki sposób kierownictwo badanych jednostek kształtuje podstawowe elementy środowiska wewnętrznego, procesy komunikacji wewnętrznej i kontroli w zakresie zapewnienia ochrony zasobów informatycznych. Badania prezentują również podejście kierownictwa jednostek do różnych aspektów zarządzania ryzykiem informatycznym oraz stosowania procedur organizacyjno-administracyjnych, zabezpieczeń fizyczno-technicznych i programowych w środowisku informatycznym rachunkowości. Problemy analizowane w artykule rozpoczynają dyskusję naukową, która powinna prowadzić do opracowywania modeli teoretycznych, wskazywania skutecznych metod i narzędzi, a także wskazywania odpowiednich inicjatyw legislacyjnych. Metody badawcze wykorzystane w opracowaniu to analiza piśmiennictwa oraz regulacji w przedmiotowym zakresie, analiza wyników badań ankietowych, dedukcja i wnioskowanie.

Słowa kluczowe: IT, bezpieczeństwo informatyczne w rachunkowości, system kontroli wewnętrznej, zarządzanie ryzykiem.

Abstract

Management of accounting information resources security in Polish entities – study results

The presence of contemporary entities in the cyber-space shows that IT offers unlimited possibilities of running a business and developing an organisation. On the other hand, it involves a greater number of

* Dr Elżbieta Izabela Szczepankiewicz, Uniwersytet Ekonomiczny w Poznaniu, Katedra Rachunkowości, elzbieta.szczepankiewicz@ue.poznan.pl

ISSN 1641-4381 *print* / ISSN 2391-677X *online*

http://www.ztr.skwp.pl
DOI: 10.5604/01.3001.0012.0379

internal and external threats in the area of accounting information resources security. The objective of the paper is to diagnose the current level of accounting information resources security (AIRS) assurance in Polish business entities. The paper analyses two research hypotheses. In accordance with the first one, the AIRS assurance level in various entity groups may be different, even though all entities should have implemented the same requirements of the Accounting Act in the analyzed area. The identified differences may result from the effect of additional, industry-specific regulations. The other hypothesis claims that in the private business area, accounting and auditing companies adhere to AIRS regulations more strictly than other small and medium enterprises. The paper defines the fundamental factors affecting the functioning of corporate accounting systems in the three dimensions of the cyber-space. Subsequently, the author presents the results of empirical research on how corporate information security is ensured in the context of internal accounting control systems and the requirements of the Polish Accounting Act. The results of the empirical research show how the management of the analysed entities crafts the basic elements of their internal environment as well as internal communication and control processes connected with ensuring information resources security. The results also show the management's approach to various aspects of risk management of accounting information resources security, as well as to adherence to organisational and administrative procedures, and to hardware and software safeguards in the IT environment of the accounting system. The issues analysed in the present paper open a scholarly discussion that should lead to the development of theoretical models, recommendation of efficient methods and tools, as well as indication of adequate legislative initiatives. Research methods used by the author include analysis of literature and legislation, analysis of survey results, deduction and inference.

Keywords: IT, security of IT resources in accounting, management control systems, risk management.

Wprowadzenie

Od kilkunastu lat jednostki gospodarcze mają bieżący dostęp do corocznych światowych raportów na temat zarządzania bezpieczeństwem informacji opracowywanych przez takie firmy jak: PwC, KPMG, Ernst & Young, Deloitte, McAfee, Centrum CSIS i inne. Badania tych firm wskazują, że głównym celem cyberataków[1] na całym świecie były i są instytucje świadczące usługi finansowe, jednak zagrożenie to w coraz większym stopniu dotyczy także innych jednostek gospodarczych. Firma PwC w swoim raporcie alarmuje, że w 2015 roku w stosunku do 2014 roku liczba incydentów bezpieczeństwa informatycznego[2] na świecie wzrosła aż o 38%, a w Polsce o ponad 46% (Raport PwC, 2016). Również z licznych doniesień prasowych wynika, że od 2014 roku w Polsce nasiliła się fala cyberataków na zasoby informatyczne rachunkowości w jednostkach gospodarczych. Wiele raportów dotyczących bezpieczeństwa informacji

[1] Według *Encyklopedii PWN* (2016) „cyberatak" to każdy rodzaj ofensywnego działania osób lub organizacji, którego celem może być zarówno system informatyczny, komputer i sieć komputerowa, jak i inne mobilne urządzenia osobiste. Cyberatak może być przeprowadzany w Internecie lub sieci wewnętrznej w samej organizacji, zwanej dalej cyberprzestrzenią, czyli przestrzeni wirtualnej, w której odbywa się komunikacja pomiędzy komputerami połączonymi siecią informatyczną, w tym siecią internetową.

[2] „Incydent dotyczący bezpieczeństwa informatycznego" to pojedyncze zdarzenie lub seria niepożądanych zdarzeń stwarzające znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażające bezpieczeństwu informacji (PN-ISO/IEC 27000). Może być związany z awarią i/lub naruszeniem ochrony informacji lub jej własności.

w jednostkach wskazuje, że cyberprzestępcy zakładają, że można łatwo wykorzystać ignorancję zarządów, a także niefrasobliwość, pośpiech, brak cierpliwości czy zwykłą niedbałość pracowników[3], które stanowią potencjalną luką bezpieczeństwa informatycznego w jednostkach. CERT Orange Polska w swoim raporcie ostrzega, aby mieć świadomość, że złośliwe oprogramowanie doprowadzające do wykonania przelewu na inne „podstawione" przez cyberprzestępcę konto bankowe, może nagle zniknąć z komputera, na którym się uaktywniło, zacierając jednocześnie ślady swojego wcześniejszego działania[4]. Odwagi cyberprzestępcom dodaje mała skuteczność wykrywania sprawców oraz niewielka liczba zgłoszeń do organów ścigania. (Raport CERT, 2016). Natomiast KPMG na podstawie z swoich badań wskazało, że tylko 29% zarządów badanych podmiotów uznało cyberbezpieczeństwo jako bardzo ważny problem, który ma obecnie i będzie miało w przyszłości największy wpływ na funkcjonowanie ich podmiotów (Raport KPMG, 2016).

Problemy zapewnienia ciągłości działania procesów w jednostce, a także zapewnienie wiarygodności danych finansowych z komputerowych ksiąg rachunkowych i ochrona zasobów informatycznych rachunkowości (ZIR) w polskich jednostkach gospodarczych stanowiły inspirację dla autorki do podjęcia badań empirycznych w tym zakresie.

Celem opracowania jest wskazanie uwarunkowań prowadzenia rachunkowości we współczesnej cyberprzestrzeni oraz diagnoza aktualnego poziomu zapewnienia bezpieczeństwa ZIR w polskich jednostkach gospodarczych. Aby zrealizować założony cel, przeprowadzono analizę światowych koncepcji kontroli wewnętrznej, a także piśmiennictwa naukowego, wyników badań oraz regulacji dotyczących problemów zapewnienia bezpieczeństwa informatycznego w jednostkach. Następnie przeprowadzono badania empiryczne w ponad 400 jednostkach na temat podstawowych aspektów organizacji systemów kontroli wewnętrznej w środowisku informatycznym, ze szczególnym uwzględnieniem ochrony ZIR w jednostkach. Do konstrukcji ankiety wykorzystano założenia światowych koncepcji kontroli wewnętrznej. Badania empiryczne w kontekście koncepcji systemu kontroli wewnętrznej w środowisku informatycznym rachunkowości zostały przeprowadzone w Polsce po raz pierwszy.

W artykule przyjęto dwie hipotezy badawcze. Pierwsza z nich stanowi, że poziom zapewnienia bezpieczeństwa ZIR w różnych grupach badanych jednostek może się znacznie różnić, pomimo że wszystkie jednostki powinny w takim sam sposób stosować

[3] Księgowi w przeciętnej firmie mogą wykonywać kilkadziesiąt (a w dużej firmie nawet kilkaset) przelewów miesięcznie. Dlatego każdy księgowy powinien zadać sobie pytanie: Czy za każdym razem analizuje się szczegółowo wszystkie dane do przelewów, w tym przelewów cyklicznych dla stałych kontrahentów?

[4] Zatem, jak w takim przypadku księgowy może udowodnić zarządowi, że doszło do cyberataku, a przelew, który wykonał został „przekierowany" przez cyberprzestępcę na postawione konto? Jak księgowy ma wytłumaczyć, że nie popełnił błędu, bo miał pewność, że widział konto prawidłowe? Albo jak ma on udowodnić, że nie wpisał celowo innego numeru konta i nie współdziałał z przestępcą?

się do wymogów ustawy o rachunkowości w przedmiotowym obszarze badania. Ewentualnie ujawnione różnice mogą wynikać z wpływu dodatkowych regulacji sektorowych, np. w zakresie zarządzania ryzykiem, kontroli wewnętrznej i innych. Dlatego badania prowadzono z uwzględnieniem podziału według grup jednostek takich, jak: instytucje finansowe, jednostki sektora finansów publicznych, jednostki w sektorze prywatnym. Z próby badawczej reprezentującej jednostki w sektorze prywatnym wyodrębniono biura rachunkowe i małe firmy audytorskie przyjmując drugą hipotezę, że podmioty te najlepiej znają obowiązujące przepisy ustawy o rachunkowości w przedmiotowym obszarze badania i prawdopodobnie bardzo restrykcyjnie, tak jak instytucje finansowe, przestrzegają przepisów dotyczących zapewnienia bezpieczeństwa danych finansowych swoich klientów.

W pierwszej części opracowania wskazano uwarunkowania prowadzenia współczesnej rachunkowości w środowisku informatycznym. Określono trzy wymiary interakcji jednostek we współczesnej cyberprzestrzeni, a także wskazano potencjalne zagrożenia dla bezpieczeństwa ZIR oraz konieczne działania dla zapewnienia skutecznej ochrony ZIR. Następnie przeprowadzono przegląd podstawowych regulacji dotyczących zapewnienia wiarygodnej informacji finansowej i bezpieczeństwa zasobów informatycznych rachunkowości w jednostkach. W dalszej części omówiono wyniki autorskich badań empirycznych, które pokazują, w jaki sposób kierownictwo badanych jednostek kształtuje podstawowe elementy kontroli wewnętrznej w obszarze rachunkowości prowadzonej w środowisku informatycznym. Badania prezentują podejście kierownictwa jednostek do kształtowania poszczególnych elementów kontroli wewnętrznej. Przede wszystkim ujawniają one poziom świadomości i wiedzy kierownictwa w obszarze identyfikacji zagrożeń, zarządzania ryzykiem oraz stosowania procedur i zabezpieczeń w środowisku informatycznym rachunkowości.

1. Rachunkowość jednostek w cyberprzestrzeni

W literaturze światowej o cyberprzestrzeni oraz zagrożeniach z nią związanych jest mowa już od ponad trzech dekad, czyli od momentu popularyzacji wykorzystania Internetu. Świadczą o tym liczne opracowania teoretyczne i empiryczne, np.: R.P. Fisher (1984),G. Siegel, J.E. Sorensen (1999), K. Mitnick, W. Simon (2002), E. J. Umble i in. (2003), R.W. Scapens i in. (2003), K.J. Knapp i in. (2009), N. Kshetri (2009), K.T. Smith i in. (2011) i wielu innych autorów. W Polsce również od ponad 20 lat publikowane są opracowania na ten temat, np.: M. Stawowski (1998), T. Kifner (1999), J.W. Wójcik (1999), E. Dudek (2003), A. Białas (2007), E.I. Szczepankiewicz, E. Dudek (2008, 2009), K. Liderman (2012), B. Zaleska, K. Dziadek (2013), J. Wasilewski (2013), Pałęga i in. (2014a, 2014b), J. Unold (2015), A. Bartoszewicz, S. Bartoszewicz (2016) i wielu innych autorów. Ale niewielu autorów przeprowadzało badania empiryczne w tym zakresie.

Pojęcie cyberprzestrzeni w ostatnich latach zostało także zdefiniowane w regulacjach prawnych wielu państw oraz na szczeblu UE. Według słownika pojęć z zakresu społeczeństwa informacyjnego Komisji Europejskiej jest to wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata (Wasilewski, 2013). Także w Polsce od kilku lat ochrona cyberprzestrzeni jest przedmiotem ciągłych prac legislacyjnych w tym zakresie. W „Rządowym Programie Ochrony Cyberprzestrzeni RP na lata 2009–2011" (2009) po raz pierwszy zdefiniowano „cyberprzestrzeń" jako „cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Natomiast cyberprzestrzeń RP należy rozumieć jako cyfrową przestrzeń stanowiącą logicznie wydzielony obszar w obrębie terytorium RP, a także w placówkach i kontyngentach RP poza terytorium kraju.

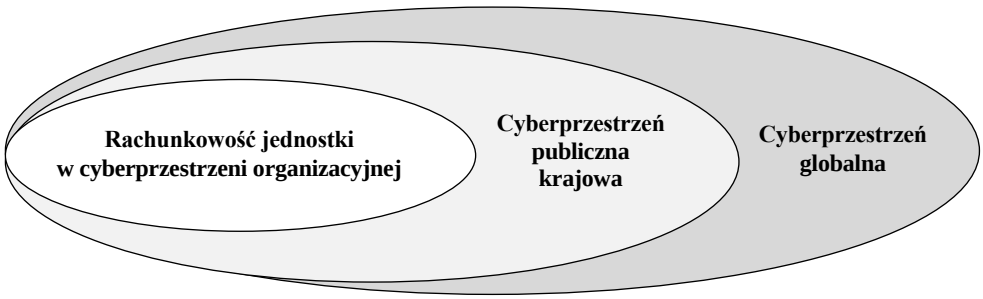
Obecnie każda, nawet najmniejsza, jednostka gospodarcza w cyberprzestrzeni kontaktuje się z jednostkami sektora finansów publicznych (np. organami podatkowymi, ZUS, GUS, KRS, innymi urzędami i organizacjami tego sektora), a także z różnymi jednostkami gospodarczymi i organizacjami, zarówno w kraju, jak i na świecie. Zatem cyberprzestrzeń dla pojedynczej jednostki gospodarczej ma nie tylko charakter organizacyjny, ale i ponadnarodowy, ponieważ jest tworzona przez systemy teleinformatyczne połączone za pośrednictwem sieci telekomunikacyjnych, których elementy infrastrukturalne są zlokalizowane na terenie innych państw. Dotyczy to także zjawiska przetwarzania i przechowywania danych, w tym danych finansowych w tzw. chmurze (*Cloud computing*)[5].

Mając powyższe na uwadze, można uznać, że współczesne działania jednostek gospodarczych polegające na gromadzeniu danych, wytwarzaniu, modyfikowaniu, odczytywaniu, przechowywaniu oraz wymianie informacji odbywają się w trzech wymiarach cyberprzestrzeni. Zdaniem autorki można wyróżnić: cyberprzestrzeń organizacyjną (przetwarzanie, przepływ i przechowywanie informacji w obrębie danej jednostki gospodarczej), cyberprzestrzeń krajową (w tym: publiczną, obejmującą interakcje jednostki z sektorem finansów publicznych i innymi interesariuszami w kraju), a w szerszej przestrzeni światowego wykorzystania Internetu także cyberprzestrzeń globalną. Relacje i zależności rachunkowości jednostki w cyberprzestrzeni organizacyjnej od cyberprzestrzeni krajowej i globalnej prezentuje rys. 1.

Ze względu na ciągłe interakcje w cyberprzestrzeni organizacyjnej, krajowej i globalnej, jednostki gospodarcze są narażone nie tylko na zagrożenia wewnętrzne (na poziomie cyberprzestrzeni organizacyjnej), ale i zewnętrzne (na poziomie cyberprzestrzeni publiczno-krajowej i globalnej). Dlatego, aby przeciwdziałać wewnętrznym i zewnętrznym zagrożeniom, kierownictwo jednostek musi podejmować określone działania zapewniające cyberbezpieczeństwo (bezpieczeństwo informatyczne) mając na uwadze każdy z tych wymiarów cyberprzestrzeni.

[5] O aspektach przetwarzania w chmurze i zagrożeniach z nimi związanych na przykład w pracach: Mell, Grance (2009), Etro (2010), Łapiński, Wyżnikiewicz (2011).

Rysunek 1. Współczesne zależności prowadzenia rachunkowości jednostki w cyberprzestrzeni organizacyjnej od cyberprzestrzeni krajowej i globalnej



Źródło: opracowanie własne.

W piśmiennictwie definicje cyberbezpieczeństwa są różne, w zależności od tego, czy odnosi się ono do indywidualnych użytkowników Internetu, przedsiębiorstw i instytucji, czy do państw (w tym struktur organizacyjnych administracji). Jednak niezależnie od wskazanego wyżej podmiotu odniesienia – indywidualny użytkownik, jednostka gospodarcza czy państwo – główną istotą tego pojęcia jest podejmowanie działań i określenie zasobów, które umożliwiają danemu podmiotowi osiągnięcie określonych celów w obszarze bezpieczeństwa informatycznego. Cyberbezpieczeństwo powinno być zapewniane w sposób niezawodny i ciągły z zachowaniem wszelkich zasad prywatności i ochrony danych w cyberprzestrzeni.

Bezpieczeństwo informatyczne w jednostce gospodarczej można zapewnić wykorzystując potencjał własnych specjalistów i/lub korzystając z zewnętrznych usług firm specjalizujących się w tym zakresie. Zewnętrzna usługa cyberbezpieczeństwa dla jednostek gospodarczych ma znacznie szerszy wymiar niż dla indywidualnych użytkowników Internetu. Obejmuje ona zapewnienie ciągłości działania procesów i funkcji biznesowych, a także ochronę danych poufnych oraz gromadzonych i przetwarzanych informacji w chmurze prywatnej i/lub publicznej.

Mając na uwadze omówione zagadnienia dotyczące funkcjonowania jednostek gospodarczych we współczesnej cyberprzestrzeni, a w szczególności zależności bezpieczeństwa informatycznego ZIR w cyberprzestrzeni organizacyjnej jednostki od cyberbezpieczeństwa w cyberprzestrzeni krajowej i globalnej (jak na rys. 1), autorka stawia tezę, że obecnie na poziomie cyberprzestrzeni organizacyjnej każdej jednostki gospodarczej szczególnych działań z zakresu zapewnienia bezpieczeństwa informatycznego wymaga ochrona ZIR[6] jednostki. Zdaniem autorki zapewnienie skutecznej ochrony ZIR wymaga następujących kompleksowych działań:

[6] Przez ZIR autorka rozumie co najmniej: system informatyczny rachunkowości SIR, czyli aplikacje użytkowe: system finansowo-księgowy i wszystkie podsystemy dziedzinowe, sprzęt komputerowy z systemem operacyjnym, pozostałą infrastrukturę techniczną i telekomunikacyjną, nośniki danych elektronicznych i bazy danych, w tym zawierające księgi rachunkowe oraz dokumentację ewidencyjną SIR (w myśl art. 10 ust. 1 pkt 3 i 4 UoR).

1) kształtowania odpowiedniego środowiska wewnętrznego i kontroli;
2) ciągłej identyfikacji zagrożeń i analizy ryzyka informatycznego;
3) przyjęcia, a następnie ciągłego dostosowywania do aktualnych warunków odpowiednich do oszacowanego ryzyka mechanizmów organizacyjno-administracyjnych, fizyczno-technicznych i programowych środków ochrony ZIR przed ryzykiem;
4) skutecznego, bieżącego komunikowania o powyższych aspektach wszystkim pracownikom jednostki.

2. Obowiązek zapewnienia wiarygodnej informacji finansowej i bezpieczeństwa zasobów informatycznych rachunkowości w jednostkach według regulacji

Opracowanie określonych regulacji prawnych i konkretne działania to podstawowy środek do zapewnienia cyberbezpieczeństwa zarówno w skali makro, jak i mikro współczesnej gospodarki (Kshertri, 2009; Barclay, 2014). Właściwe regulacje, ich wdrożenie oraz egzekwowanie, mają wpływ na zwiększenie zarówno bezpieczeństwa informatycznego pojedynczych podmiotów, jak i krajowych instytucji publicznych oraz światowych organizacji i instytucji, np. giełd.

W Polsce, podobnie jak w innych krajach, podjęto szereg działań i prac legislacyjnych w zakresie zapewnienia wiarygodności informacji finansowej z komputerowych ksiąg rachunkowych i ochrony ZIR w jednostkach. Wymagania w tym zakresie po raz pierwszy uregulowała ustawa o rachunkowości (UoR), która zaczęła obowiązywać od 1995 roku (Ustawa z 29.09.1994 r.). W 2001 roku podczas kolejnej nowelizacji UoR znacznie poszerzono te wymagania. Stały się one przedmiotem licznych opracowań i dyskusji teoretyków (np. Dziedziczak, Stępniewski, 1999; Dudek 2002a, 2002b, 2002c; Andrzejewski i in., 2004), a także artykułów praktyków w czasopismach specjalistycznych dla księgowych. W kolejnej nowelizacji UoR z 2009 roku poprawiono niektóre przepisy oraz wprowadzono dodatkowe zapisy w tym zakresie, dostosowujące wymagania do aktualnego rozwoju technologicznego (Luty i in., 2010; Zaleska, 2011a, 2011b; Kunz, Tymińska, 2014). Nadal jednak nie wyjaśniono wielu pojęć, a niektóre zapisy wśród teoretyków i praktyków budziły dalsze wątpliwości. Z tego względu w 2010 roku Komitet Standardów Rachunkowości (KSR) wydał do UoR stanowisko w sprawie niektórych zasad prowadzenia ksiąg rachunkowych (Komunikat nr 10 z 18.05.2010 r.). W tym kilkunastostronicowym dokumencie zdefiniowano niektóre pojęcia i wyjaśniono podstawowe zasady prowadzenia komputerowych ksiąg rachunkowych po nowelizacji UoR.

Obecnie, zdaniem autorki, kierownicy jednostek i księgowi dla zapewnienia wiarygodności danych i skutecznej ochrony ZIR w cyberprzestrzeni, zarówno na etapie projektowania systemów informatycznych rachunkowości (SIR), jak i ich eksploatacji, powinni przestrzegać co najmniej art. 10, 12–18, 20–25, 71–75 UoR w myśl zasad określonych w cytowanym stanowisku KSR z 2010 roku.

Jak wcześniej wspomniano, bezpieczeństwo informatyczne w jednostkach gospodarczych wiąże się również z interakcjami jednostek w cyberprzestrzeni publicznej. Od kilku lat jednostki gospodarcze w Polsce mogą przesyłać deklaracje ubezpieczeniowe do ZUS w wersji elektronicznej przy pomocy programu e-płatnik (Rozporządzenie z 9.09.2013 r.). Od 1 stycznia 2015 roku płatnicy i podatnicy są zobowiązani do przesyłania w formie elektronicznej do urzędów skarbowych większości deklaracji podatkowych (w tym, CIT-8, PIT-11, PIT-4R, PIT-8AR) (Ustawa z 14.09.2014 r.). Mogą oni również w formie elektronicznej przesyłać rozliczenia roczne PIT oraz deklaracje VAT. Od lipca 2016 roku zobowiązano duże jednostki do udostępniano podatkowym organom kontroli w postaci elektronicznej jednolitych plików kontrolnych (JPK)[7] zawierających informacje z ksiąg rachunkowych jednostki (*Ordynacja podatkowa*, 2015). W kolejnych okresach obowiązkiem przesyłania JPK objęto również średnie, małe, a nawet mikrojednostki będące podatnikami VAT. W przyszłości wszystkie jednostki będą zobowiązane do przesyłania w tej formie również sprawozdań finansowych. Również kilkakrotnie zmieniano ustawę o ochronie danych osobowych (Ustawa z 29.09.1997 r.), której przepisy dotyczą także informacji przetwarzanych w SIR. Wkrótce polskie jednostki będą musiały się stosować także do przepisów unijnego rozporządzenia o danych osobowych (RODO – Rozporządzenie UE 2016/679 z 27.04.2016 r.). Od 1 kwietnia 2016 r. zmieniły się także zasady bezpiecznego przesyłania e-wniosków do sądów rejestrowych, które od tego momentu muszą być opatrzone podpisem potwierdzonym profilem zaufanym ePUAP (Ustawa z 28.11.2014 r.; Ustawa z 17.11.1964 r.). W przyszłości wszystkie wnioski, a także sprawozdania finansowe do KRS będzie należało składać w formie elektronicznej[8].

Niektóre jednostki są zobowiązane do stosowania regulacji sektorowych mających wpływ na bezpieczeństwo ZIR. Na przykład w jednostkach sektora finansów publicznych w 2003 roku wprowadzono Standardy kontroli finansowej (2003), obejmujące „Mechanizmy kontroli systemów informatycznych" opisane w Standardach nr 19–24. Od 2010 roku w tym sektorze zaczęły obowiązywać Standardy kontroli zarządczej (2009), w których zagadnienia ze Standardów 19–24 przeniesiono do jednego Standardu nr 15 „Mechanizmy kontroli dotyczące systemów informatycznych". W 2012 roku Minister Finansów ogłosił komunikat w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem (2012). Na podstawie wytycznych z tych regulacji w jednostkach sektora finansów publicznych projektowano systemy kontroli wewnętrznej, w tym mechanizmy w obszarze bezpieczeństwa systemów informatycznych.

[7] JPK w 2010 r. zdefiniowała OECD i wskazała format przesyłanych danych XML. W Polsce nie korzysta się z tego formatu, JPK mogą być przesyłane w formacie UBL lub XBRL, które szerzej opisują Ramin i Reiman (2013). Należy podkreślić, że w poprzednich latach JPK wprowadzono już w kilku krajach UE.

[8] Przytoczone przepisy odnoszą się bezpośrednio do przedmiotowych zagadnień, ale nie wyczerpują one listy regulacji, które można wskazać, jako ważne dla zapewnienia bezpieczeństwa informatycznego. Ze względu na ograniczoną objętość opracowania celowo pominięto dyrektywy UE, inne polskie ustawy, rozporządzenia, standardy ISO, COSO (1994), standardy kontroli zarządczej. Omawia je Szczepankiewicz (2016).

Natomiast w sektorze prywatnym tylko w bankach obowiązują regulacje sektorowe w tym zakresie. Obecnie banki stosują się do trzeciej wersji Rekomendacji D, która dotyczy zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego (2013). Zastąpiła ona poprzednią Rekomendację D z 2002 roku (pierwsza była ogłoszona w 1997 r.). W bankach obowiązuje również trzecia wersja Rekomendacji H, która dotyczy kontroli wewnętrznej (2011). Poprzednie wersje tej Rekomendacji H były ogłoszone w latach 1999 i 2002. Rekomendacja D i H dostarcza bankom ogólne wytyczne przydatne do projektowania i doskonalenia systemu kontroli wewnętrznej w środowisku informatycznym. Należy podkreślić, że w innych instytucjach finansowych nie ustanowiono dotychczas podobnych regulacji w przedmiotowym zakresie.

3. Problemy zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości w cyberprzestrzeni jednostek – wyniki badań

3.1. Metodyka badania i opis próby badawczej

Autorka od lutego 2014 roku do stycznia 2016 roku przeprowadziła pierwsze w kraju[9] badania empiryczne dotyczące podstawowych aspektów organizacji systemów kontroli wewnętrznej w środowisku informatycznym[10], ze szczególnym uwzględnieniem ochrony ZIR w jednostkach[11], aplikując do tego celu podstawowe założenia światowej koncepcji kontroli wewnętrznej COSO (1994) i COSO II (2004).

Próbę badawczą stanowiły następujące podmioty[12]:

1) jednostki samorządu terytorialnego, reprezentujące sektor finansów publicznych;
2) instytucje finansowe;

[9] Autorka dokonując przeglądu literatury oraz raportów na temat bezpieczeństwa informacji w polskich jednostkach nie znalazła badań empirycznych na temat jakości systemów zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości w kontekście organizacji systemów kontroli wewnętrznej w środowisku informatycznym oraz w świetle wymagań stawianych przez UoR.

[10] Bezpośrednim celem badania było otrzymanie wyników empirycznych, na podstawie których można będzie sformułować cel, tezę oraz przeprowadzić rozważania w monografii autorki pt: *Audyt kontroli wewnętrznej rachunkowości w środowisku informatycznym*. Monografia ukazała się pod koniec 2016 r. w wydawnictwie DIFIN. Szczegółowe wyniki badań prezentowane w niniejszym artykule nie były prezentowane w tej monografii, a jedynie wnioski ogólne, stanowiąc tło dla prowadzonych rozważań z punktu widzenia poprawy jakości rewizji finansowej i audytu wewnętrznego w środowisku informatycznym rachunkowości.

[11] Autorka musiała zapewnić ankietowanych o zachowaniu pełnej anonimowości i poufności danych o podmiotach oraz o ich działaniach z zakresu bezpieczeństwa zasobów informatycznych ujawnianych w ankiecie.

[12] Pierwsze badania własne autorka, jako członek zarządu SKwP Oddział w Poznaniu, 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: SKwP, Oddział w Poznaniu i enova dla biznesu. Kolejne badania zostały przeprowadzone podczas dwóch konferencji dla księgowych w 2015 r. i 2016 r., a także z wykorzystaniem listy mailingowej członków SKwP O/Poznań i prywatnych kontaktów zawodowych autorki jako audytora wewnętrznego.

3) firmy prywatne prowadzące rachunkowość na podstawie przepisów UoR (o różnych wielkościach, formach własności, reprezentujące różne branże).

W jednostkach samorządu terytorialnego anonimowe ankiety skierowano do kierowników i pracowników wydziałów/działów finansowych oraz audytorów wewnętrznych w tych jednostkach[13]. W jednostkach poza sektorem finansów publicznych anonimowe ankiety wypełniali pracownicy działów finansowo-księgowych, pracownicy administracji oraz audytorzy wewnętrzni i zewnętrzni. Ogółem zwrot prawidłowych ankiet przydatnych do analizy uzyskano z 415 jednostek, które sklasyfikowano w tabeli 1.

Tabela 1. Prezentacja jednostek biorących udział w badaniach empirycznych

Klasyfikacja jednostek w próbie badawczej	**Liczba**
JST – jednostki samorządu terytorialnego	106
IF – instytucje finansowe (banki komercyjne i spółdzielcze oraz zakłady ubezpieczeń) *	14
BRiFA – biura rachunkowe oraz małe, lokalne firmy audytorskie**	29
FP 20 – firmy prywatne zatrudniające do 20 osób	86
FP 100 – firmy prywatne zatrudniające od 21–100 osób	68
FP>100 – firmy prywatne zatrudniające powyżej 100 osób	112
Razem	415

* Z uwagi na to, że wyniki z ankiet uzyskanych z banków i zakładów ubezpieczeń są podobne, wykazano je w jednej kolumnie. Autorka, znając regulacje dotyczące banków (w tym: Rekomendacja D i H) i zakładów ubezpieczeń (Standard zarządzania ryzykiem), uznała, że podobne wyniki w tych podmiotach mogą wynikać z restrykcyjnych regulacji w zakresie kontroli wewnętrznej, zarządzania ryzykiem i bezpieczeństwem informacji.

** Z próby badawczej reprezentującej jednostki w sektorze prywatnym wyodrębniono biura rachunkowe i małe firmy audytorskie. Takie wyodrębnienie autorka uznała za ważne, przyjmując hipotezę, że podmioty te najlepiej znają obowiązujące regulacje w przedmiotowym zakresie badania i prawdopodobnie restrykcyjnie przestrzegają przepisów dotyczących zapewnienia bezpieczeństwa danych finansowych swoich klientów. Badanie podmioty w tej grupie zatrudniały nie więcej niż 20 osób.

Źródło: opracowanie własne.

Ponadto w wybranych jednostkach przeprowadzono wywiady osobiste, które dotyczyły różnych aspektów stosowania określonych rozwiązań w zakresie bezpieczeństwa informatycznego.

Prezentację wyników przeprowadzono w następujących obszarach systemu kontroli wewnętrznej (według COSO i COSO II) w środowisku informatycznym, które mają

[13] Szczegółowe wyniki badań w jednostkach sektora finansów publicznych autorka zaprezentowała w monografii: *Kontrola zarządcza w jednostkach samorządu terytorialnego. Ocena i doskonalenie kontroli zarządczej w środowisku informatycznym rachunkowości*. UE i Wydawnictwo Naukowe CONTACT, Poznań, wydania: 2016 i 2017. Dlatego szczegółowe wyniki uzyskane z jednostek samorządu terytorialnego będą prezentowane jedynie wybiórczo, w kontekście porównań z sektorem prywatnym.

wpływ na właściwe zapewnienie bezpieczeństwa ZIR w badanych jednostkach, a mianowicie:
1) kształtowanie środowiska wewnętrznego i kontroli oraz komunikacja wewnętrzna;
2) podejście do identyfikacji, analizy i postępowania z ryzykiem;
3) stosowanie mechanizmów organizacyjno-administracyjnych oraz zabezpieczeń fizyczno-technicznych i programowych.

Wyniki badań na podstawie pytań ankietowych, które skierowano do pracowników komórek organizacyjnych w badanych grupach jednostek zaprezentowano w tabelach 1–4.

3.2. Kształtowanie środowiska wewnętrznego i kontroli oraz komunikacja w obszarze zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości

Właściwe kształtowanie środowiska wewnętrznego i kontroli oraz skuteczna komunikacja wewnętrzna w jednostce w sposób zasadniczy wpływa na jakość zapewnienia bezpieczeństwa ZIR. W koncepcji kontroli wewnętrznej według COSO i COSO II, standardach audytu wewnętrznego, standardach rewizji finansowej oraz standardach kontroli zarządczej wymieniono takie ogólne elementy środowiska wewnętrznego jak: promowanie i przestrzeganie wartości etycznych, zapewnienie w jednostce pracowników o odpowiednich kwalifikacjach, właściwe ukształtowanie struktury organizacyjnej z podziałem, uprawnień, obowiązków, odpowiedzialności i skutecznym delegowaniem uprawnień według kompetencji i bieżących potrzeb organizacji. Są zarówno „miękkie" jak i „twarde" elementy zarządzania organizacjami.

Każdy z tych ogólnych elementów w szczególny sposób odnosi się do problemów zapewnienia bezpieczeństwa ZIR w jednostce. Na przykład kierownictwo powinno wspierać i promować wśród pracowników przestrzeganie wartości etycznych. Kierownictwo i pracownicy, którzy wspólnie zdefiniowali, a następnie świadomie przyjęli w jednostce określone wartości etyczne i reguły postępowania oraz przestrzegają je przy wykonywaniu powierzonych zadań, nie będą narażali jednostki na utratę czy zniszczenie ZIR. Szczególna rola kierownictwa w tym zakresie polega na dawaniu dobrego przykładu w swoim codziennym postępowaniu i podejmowaniu decyzji. Niedbałe postępowanie i szkody nawet, jeśli były wyrządzone nieświadomie, przez jakiegokolwiek członka organizacji, powinny być odpowiednio piętnowane. Wymagałoby to również wdrożenia odpowiednich procedur organizacyjno-administracyjnych, które ograniczyłyby występowanie nieprawidłowości wynikających z niedbalstwa czy celowego działania. Niezbędna jest także skuteczna komunikacja wewnętrzna w pracownikami oraz bieżący nadzór i kontrola.

Kierownictwo musi także zadbać, aby każda osoba w organizacji posiadała stosowną wiedzę, umiejętności i doświadczenie pozwalające skutecznie i efektywnie wypełniać powierzone jej zadania na danym stanowisku, w tym z zakresu ochrony ZIR. Dlatego

już sam proces zatrudnienia powinien być prowadzony w sposób zapewniający wybór najlepszego kandydata na dane stanowisko pracy. Jednostka w okresie zatrudnienia na danym stanowisku powinna zapewnić rozwój kompetencji zawodowych wymaganych do skutecznego zapewnienia ochrony ZIR.

Struktura organizacyjna jednostki powinna być dostosowana do aktualnych celów i zadań jednostki, w tym z zakresu ochrony ZIR. Dlatego zakresy zadań, uprawnień i odpowiedzialności komórek organizacyjnych, zespołów i poszczególnych pracowników oraz podległość i relacje służbowe pracowników powinny być określone w formie pisemnej w sposób kompletny, przejrzysty i spójny. Należy również precyzyjnie określić zakres uprawnień delegowanych poszczególnym kierownikom i pracownikom. Niezbędne jest także określenie sposobu kontroli realizacji tych uprawnień, odpowiednio do wagi i stopnia skomplikowania podejmowanych decyzji oraz ryzyka z nimi związanego.

Badanie kształtowania środowiska wewnętrznego i kontroli oraz komunikacji wewnętrznej w jednostkach jest bardzo skomplikowane ze względu na występowanie wielu „miękkich" czynników organizacyjnych. Ich ocena przez danego ankietowanego może być obarczona dużym współczynnikiem subiektywności. Dlatego, w celu uzyskania odpowiedzi na temat kształtowania środowiska wewnętrznego i kontroli oraz komunikacji wewnętrznej w obszarze zapewnienia bezpieczeństwa ZIR w jednostkach badano następujące zagadnienia:

- Czy pracownicy biorą udział w wystarczającym stopniu w szkoleniach z zakresu ochrony zasobów informatycznych (aspekty kwalifikacji i etyki)?
- Czy pracownicy mają bieżący dostęp do procedur/instrukcji w zakresie ochrony ZIR obowiązujących w jednostce (aspekt skutecznej komunikacji wewnętrznej)?
- Czy pracownicy wiedzą jak postępować w przypadku wystąpienia sytuacji nadzwyczajnej, na przykład pożaru, zalania, poważnej awarii systemu informatycznego (aspekt skutecznej komunikacji wewnętrznej)?
- Czy postawa osób na stanowiskach kierowniczych w komórce organizacyjnej zachęca pracowników do sygnalizowania problemów i zagrożeń informatycznych przy realizacji zadań komórki organizacyjnej (aspekty etyki i nadzoru bieżącego)?
- Czy przełożeni na co dzień zwracają wystarczającą uwagą na przestrzeganie przez pracowników zasad, procedur, instrukcji, itp. obowiązujących w jednostce (aspekty etyki i nadzoru bieżącego)?

Na podstawie uzyskanych wyników, należy stwierdzić, że spośród wszystkich badanych podmiotów średnio 57% ankietowanych uważało, że bierze udział w wystarczającym stopniu w szkoleniach, aby skutecznie realizować powierzone zadania z zakresu ochrony zasobów informatycznych. Przeprowadzając bardziej szczegółową analizę udzielonych odpowiedzi można stwierdzić, że tylko wyniki ankiet z IF oraz BRiA znacznie przekroczyły ten poziom odpowiedzi. Poniżej średniej znalazły się wyniki uzyskane z jednostek samorządu terytorialnego oraz firm z sektora prywatnego zatrudniających do 100 osób.

W badanych podmiotach średnio 66% ankietowanych ma bieżący dostęp do procedur/instrukcji w zakresie ochrony ZIR obowiązujących w jednostce, na przykład poprzez intranet. Znacznie wyższe wyniki od średniej uzyskano na podstawie odpowiedzi z IF, JST oraz FP zatrudniających powyżej 100 osób. Duże podmioty mają opracowane procedury i sformalizowane systemy komunikacji wewnętrznej z pracownikami. Jednak analizując tylko sektor prywatny, poza BRiA, średnio 52% pracowników ma bieżący dostęp do procedur/instrukcji w zakresie ochrony ZIR obowiązujących w jednostkach.

Średnio 85% ankietowanych wie jak postępować w przypadku wystąpienia sytuacji nadzwyczajnej, na przykład pożaru, zalania, poważnej awarii systemu informatycznego w swojej jednostce. W tym przypadku odpowiedzi z poszczególnych grup podmiotów odbiegały od średniej *in minus* maksymalnie o 8%. Jednak analizując tylko sektor prywatny, poza BRiA, średnio 83% pracowników wie jak postępować w przypadku wystąpienia sytuacji nadzwyczajnej, na przykład poważnej awarii systemu informatycznego w jednostce. Podobny wynik uzyskano również w JST.

Kolejne pytanie dotyczyło tzw. „miękkich" czynników organizacyjnych, czyli relacji między pracownikami i przełożonymi w kwestii podejścia do ochrony zasobów informatycznych. Dlatego te wyniki mogą być obarczone odczuciami subiektywnymi ankietowanych. Wyniki wskazują, że średnio w 75% badanych podmiotów postawa osób na stanowiskach kierowniczych zachęca pracowników do sygnalizowania problemów i zagrożeń informatycznych przy realizacji zadań komórki organizacyjnej. Poniżej średniej znalazły się odpowiedzi z JST oraz małych FP zatrudniających do 20 pracowników.

W odpowiedzi na pytanie, czy przełożeni na bieżąco zwracają wystarczającą uwagą na przestrzeganie przez pracowników zasad, procedur i instrukcji obowiązujących w jednostce uzyskano średni wynik na poziomie 66%. Tylko w IF, BRiA wynik ten został znacznie przekroczony. W przypadku pozostałych podmiotów wyniki były znacznie niższe od średniej.

Szczegółowe wyniki badań empirycznych w zakresie kształtowania środowiska wewnętrznego i kontroli w obszarze zapewnienia bezpieczeństwa ZIR w jednostkach przedstawione zostały w tabeli 2.

Tabela 2. Kształtowanie środowiska wewnętrznego i kontroli oraz komunikacji wewnętrznej w obszarze zapewnienia bezpieczeństwa ZIR w badanych jednostkach

Pytanie	Odpowiedzi tak (dane w %)						
	JST	IF	BR i A	FP 20	FP 100	FP >100	Średnia
1. Czy bierze Pani/Pan udział w wystarczającym stopniu w szkoleniach, aby skutecznie realizować powierzone zadania z zakresu ochrony zasobów informatycznych?	50	94	86	9	44	61	57

ciąg dalszy tab. 1

Pytanie	Odpowiedzi tak (dane w %)						
	JST	IF	BR i A	FP 20	FP 100	FP >100	Średnia
2. Czy ma Pani/Pan bieżący dostęp do procedur/instrukcji w zakresie ochrony ZIR obowiązujących w jednostce (np. poprzez intranet)?	86	94	62	26	57	73	66
3. Czy wie Pani/Pan jak postępować w przypadku wystąpienia sytuacji nadzwyczajnej, np. pożaru, zalania, poważnej awarii systemu informatycznego?	83	94	86	77	89	82	85
4. Czy postawa osób na stanowiskach kierowniczych w Pani/Pana komórce organizacyjnej zachęca pracowników do sygnalizowania problemów i zagrożeń informatycznych przy realizacji zadań komórki organizacyjnej?	65	86	97	52	76	75	75
5. Czy przełożeni na co dzień zwracają wystarczającą uwagą na przestrzeganie przez pracowników zasad, procedur, instrukcji itp. obowiązujących w jednostce?	53	100	93	32	53	64	66

Źródło: opracowanie własne.

3.3. Podejście do identyfikacji, analizy i postępowania z ryzykiem w obszarze zapewnienia zasobów informatycznych rachunkowości

Jasne określenie celów i zadań w obszarze zapewnienia ochrony ZIR sprzyja efektywnemu zarządzaniu ryzykiem informatycznym. Zarządzanie ryzykiem obejmuje identyfikację czynników i zagrożeń, analizę i ustalenie sposobów postępowania z ryzykiem. Świadome zarządzanie ryzykiem ma na celu zwiększenie prawdopodobieństwa osiągnięcia celów i realizacji zadań z zakresu bezpieczeństwa informatycznego. Dlatego proces zarządzania ryzykiem powinien być dokumentowany.

Badanie obszaru zarządzania ryzykiem informatycznym w jednostkach jest mniej skomplikowane ze względu na występowanie wielu „twardych" uwarunkowań tego procesu w jednostce. W celu uzyskania odpowiedzi na temat podejścia do identyfikacji, analizy i postępowania z ryzykiem w obszarze zapewnienia bezpieczeństwa informatycznego w jednostkach zbadano następujące zagadnienia:

- Czy w jednostkach systematycznie, w udokumentowany sposób identyfikuje się zagrożenia informatyczne, które mogą przeszkodzić w realizacji celów i zadań jednostki (etap identyfikacji ryzyka)?
- Czy wśród zidentyfikowanych zagrożeń informatycznych wskazuje się istotne zagrożenia, które w znaczący sposób mogą przeszkodzić w realizacji celów i zadań jednostki (etap analizy ryzyka)?

– Czy w jednostce podejmuje się wystarczające działania mające na celu ograniczenie zidentyfikowanych zagrożeń informatycznych, w szczególności tych istotnych (etap postępowania z ryzykiem)?

Na podstawie uzyskanych wyników, należy stwierdzić, że spośród wszystkich badanych podmiotów średnio 42% podmiotów systematycznie, w udokumentowany sposób, identyfikuje zagrożenia informatyczne, które mogą przeszkodzić w realizacji celów i zadań jednostki. Znacznie powyżej średniej kształtuje się wynik badań uzyskany w IF (86%), bowiem banki i zakłady ubezpieczeń mają formalny obowiązek prowadzenia analizy ryzyka, w tym ryzyka informatycznego. Obowiązek identyfikacji i dokumentowania ryzyka formalnie dotyczy także jednostek sektora finansów publicznych. Jednak wyniki badań wskazują, że tylko nieco ponad 48% ankietowanych z JST zadeklarowało przeprowadzanie takich działań. W jednostkach z sektora prywatnego identyfikację zagrożeń informatycznych przeprowadza się fakultatywnie. W sektorze prywatnym, poza BRiA, systematyczną identyfikację ryzyka informatycznego przeprowadza średnio tylko 23% jednostek.

Wśród podmiotów, które przeprowadziły identyfikację zagrożeń informatycznych, średnio 53% podmiotów po zidentyfikowaniu czynników i zagrożeń informatycznych przeprowadza ich klasyfikację i wskazuje zagrożenia istotne, które w znaczący sposób mogą przeszkodzić w realizacji celów i zadań jednostki. Tylko odsetek wśród IF znacznie przekracza tą średnią i wynosi nieco ponad 80%. Natomiast odsetek w jednostkach sektora prywatnego jest znacznie niższy od średniej i nie przekracza 45%. Jeśli wyniki te interpretować łącznie z wynikiem 42% jednostek systematycznie przeprowadzających identyfikację ryzyka, to należałoby stwierdzić, że tylko około 19% firm potrafi klasyfikować czynniki i zagrożenia oraz zidentyfikować ryzyko istotne, dla którego należy szczególnie starannie dobierać mechanizmy kontroli i ochrony zasobów informatycznych.

Na podstawie dalszych odpowiedzi ankietowanych należy stwierdzić, że mniej niż w połowie badanych podmiotów (średnio 49%) podejmuje się wystarczające działania mające na celu ograniczenie zidentyfikowanych zagrożeń informatycznych, w szczególności tych istotnych. Sytuacja ta nie dotyczy IF, bowiem ich wynik kształtował się na poziomie 94%, w tym dla banków – 100%. Szczególnie sytuacja w jednostkach sektora prywatnego wskazuje, że w odpowiedzialność w obszarze kontroli i nadzoru w tym zakresie nie jest zadawalająca. Tylko 36% jednostek w sektorze prywatnym, poza BRiA, podejmuje wystarczające działania mające na celu ograniczenie zidentyfikowanych zagrożeń informatycznych. Jeśli wyniki te interpretować łącznie z wynikiem 42% jednostek systematycznie przeprowadzających identyfikację ryzyka, to należałoby stwierdzić, że tylko około 15% firm potrafi skutecznie zarządzać ryzykiem, czyli identyfikować, analizować ryzyko i postępować z ryzykiem, wdrażając jakiekolwiek mechanizmy ochrony przed ryzykiem.

Szczegółowe wyniki badań empirycznych na temat podejścia do identyfikacji, analizy i postępowania z ryzykiem, czyli zarządzania ryzykiem w obszarze zapewnienia bezpieczeństwa informatycznego w jednostkach zaprezentowana w tabeli 3.

Tabela 3. Podejście do zarządzania ryzykiem w obszarze zapewnienia bezpieczeństwa informatycznego w badanych jednostkach

Pytanie	Odpowiedzi tak (dane w %)						
	JST	**IF**	**BR i A**	**FP 20**	**FP 100**	**FP >100**	**Średnia**
1. Czy w Pani/Pana komórce organizacyjnej systematycznie, w udokumentowany sposób identyfikuje się zagrożenia informatyczne, które mogą przeszkodzić w realizacji celów i zadań komórki organizacyjnej (np. przez sporządzanie rejestru ryzyka lub innego dokumentu zawierającego zidentyfikowane zagrożenia/ryzyka)?	48	86	45	12	24	35	42
2. Czy wśród zidentyfikowanych zagrożeń informatycznych wskazuje się istotne zagrożenia, które w znaczący sposób mogą przeszkodzić w realizacji celów i zadań komórki organizacyjnej?	55	80	48	34	47	52	53
3. Czy w Pani/Pana komórce organizacyjnej podejmuje się wystarczające działania mające na celu ograniczenie zidentyfikowanych zagrożeń informatycznych, w szczególności tych istotnych?	43	94	48	26	39	42	49

Źródło: opracowanie własne.

3.4. Stosowanie procedur organizacyjno-administracyjnych oraz zabezpieczeń fizyczno-technicznych i programowych w obszarze zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości

Skuteczne, wydajne i adekwatne mechanizmy kontroli, czyli procedury organizacyjno-administracyjne, zabezpieczenia fizyczno-techniczne i programowe, powinny stanowić odpowiedź na konkretne zidentyfikowane ryzyko. Koszty wdrożenia i stosowania takich mechanizmów kontroli nie powinny być wyższe niż uzyskane dzięki nim korzyści. Dlatego w pierwszej kolejności należy wdrażać mechanizmy kontroli dla zniwelowania zidentyfikowanych istotnych zagrożeń dla ZIR. Ten obszar zarządzania również obejmuje wiele „twardych" elementów organizacji.

W celu uzyskania odpowiedzi na temat stosowania procedur organizacyjno-administracyjnych oraz zabezpieczeń fizyczno-technicznych i programowych w obszarze zapewnienia bezpieczeństwa informatycznego w jednostkach badano następujące zagadnienia:

– Czy w jednostce opracowano dokumenty (procedury, instrukcje, szczegółowe polityki) opisujące system bezpieczeństwa danych informatycznych, a w szczególności procedury awaryjne dla SIR?

- Czy obowiązujące procedury/instrukcje w zakresie ochrony ZIR są aktualne, tzn. zgodne z obowiązującymi przepisami prawa (w szczególności UoR) i regulacjami wewnętrznymi?
- Czy dokumenty i inne zasoby informatyczne są odpowiednio chronione przed utratą lub zniszczeniem?
- Czy w jednostce w regularnych odstępach czasu tworzy się rezerwowe kopie danych oraz przechowuje się je w wydzielonych i zabezpieczonych pomieszczenia dla tego celu?
- Czy w jednostce jest procedura przydzielania użytkownikom systemów uprawnień do danych, funkcji programów i komputerów oraz czy aplikacje SIR wymuszają okresową zmianę hasła przez użytkownika?
- Czy organizowane są szkolenia dla nowozatrudnionych pracowników w zakresie bezpieczeństwa danych informatycznych?
- Czy w jednostce stosuje się procedury i zabezpieczenia przed pozyskaniem danych informatycznych wobec osób i firm współpracujących, np. firm sprzątających, serwisu informatycznego itd.?
- Czy jednostka stosuje zapasowe źródła zasilania sprzętu informatycznego oraz czy w jednostce wyodrębniono specjalne strefy bezpieczeństwa, takie jak na przykład: serwerownia, archiwum przechowywania danych itp.?
- Czy w jednostce przeprowadza się okresową weryfikację legalności oprogramowania zainstalowanego na komputerach?

Średnio w 66% badanych podmiotów opracowano dokumenty (procedury, instrukcje, szczegółowe polityki) opisujące system bezpieczeństwa danych informatycznych. Najwyższe wyniki uzyskano w IF – wynik równy 100%, a najniższe w małych firmach, zatrudniających do 20 osób – wynik na poziomie 35%. Natomiast szczegółowe procedury awaryjne dla SIR opracowało średnio 53% badanych podmiotów. Analogicznie jak w przypadku poprzedniego pytania najwyższy wynik uzyskano w IF, a najniższy w małych firmach.

Na pytanie, czy obowiązujące procedury/instrukcje w zakresie ochrony ZIR są aktualne, tzn. zgodne z obowiązującymi przepisami prawa i regulacjami wewnętrznymi, pozytywnie odpowiedziało średnio 70% badanych. Analizując bardziej szczegółowo te odpowiedzi, w IF uzyskano 100% pozytywnych odpowiedzi, w BRiA – 93 %, JST - 79%, a w pozostałych jednostkach prywatnych średnio około 50%. Tylko 34% ankietowanych z małych firm i 44% z firm do 100 osób zatrudnionych uważa, że dysponuje aktualnymi dokumentami w tym zakresie.

Kolejna kwestia to ochrona dokumentów i innych ZIR przed utratą lub zniszczeniem. Zdaniem ankietowanych w IF w 100% zapewnia się taką ochronę. W pozostałych jednostkach, niezależnie od sektora, z wyłączeniem IF, odpowiedzi pozytywne wynosiły średnio około 67%. Tylko w małych firmach uzyskano odpowiedzi na poziomie 46%.

Średnio 76% badanych podmiotów w regularnych odstępach czasu tworzy się rezerwowe kopie danych, 58 % przechowuje się je w wydzielonych i zabezpieczonych

pomieszczenia dla tego celu. Tylko od badanych IF uzyskano pozytywne odpowiedzi na poziomie 100%. Wiele punktów poniżej tych średnich klasyfikują się małe i średnie firmy. Więcej niż połowa małych i średnich badanych jednostek, niezależnie od sektora, który reprezentuje przechowuje kopie rezerwowe w tych samych pomieszczeniach co komputery, na których tworzono kopie. Tylko duże i większość średnich jednostek ma specjalne procedury dotyczące przechowywania rezerwowych kopii danych w wydzielonych i zabezpieczonych pomieszczeniach dla tego celu, a banki przenoszą je do oddziałów zewnętrznych i/lub korzystają z usług specjalistycznych centrów przetwarzania danych. W mniejszych firmach problem przechowywania kopii rezerwowych w wydzielonych i zabezpieczonych pomieszczenia dla tego celu może być uzasadniony ze względów organizacyjnych (lokalowych).

W większości badanych jednostek (średnio 78%) aplikacje SIR wymuszają okresową zmianę hasła przez użytkowników. Jedynie w większości małych jednostek sektora prywatnego (aż 62%) nie przestrzega się tej zasady. Wynika to z dwóch sytuacji: niektóre systemy informatyczne do obsługi rachunkowości mniejszych jednostek nie zostały wyposażone w funkcje przypominania zmiany hasła lub użytkownik systemu może ręcznie zmienić datę kolejnej zmiany hasła.

W większości badanych średnich i dużych jednostek, niezależnie od sektora, funkcjonuje procedura przydzielania poszczególnym użytkownikom uprawnień do danych, funkcji programów i komputerów (w IF – 100%). Zjawisko to nie dotyczy głównie małych jednostek, gdzie zatrudnia się mniejszą liczbę księgowych, którzy mają najczęściej pełne uprawnienia do obsługi systemu. Tylko w 21% tych firm funkcjonuje taka procedura.

Zdecydowana większość małych i średnich jednostek w sektorze prywatnym oraz w JST nie organizuje żadnych szkoleń dla nowozatrudnionych pracowników w zakresie bezpieczeństwa danych informatycznych. Odpowiedzi szczegółowe ankietowanych wskazywały, że w większości jednostek pracownik uczestniczył w takim szkoleniu jeden raz w ciągu ostatnich pięciu lat.

W większości jednostek z sektora prywatnego (średnio 64%) nie stosuje się żadnych procedur i zabezpieczeń przed pozyskaniem danych informatycznych wobec osób i firm współpracujących. Problem ten wynika z nieuzasadnionego zaufania do usług serwisowych świadczonych przez firmy zewnętrzne oraz nieuświadomienia sobie zagrożeń w tym zakresie przez kierownictwo jednostki.

W 100% IF i w większości badanych jednostek stosuje zapasowe źródła zasilania sprzętu informatycznego. Odpowiedzi szczegółowe ankietowanych wskazywały, że do serwerów stosuje się UPS lub inne zaawansowane technologie podtrzymania zasilania. Na stanowiskach pracy podłączenie sprzętu komputerowego do zasilania następuje zazwyczaj przez listwę zasilającą z bezpiecznikami i tańsze zasilacze UPS. Tylko 46% małych firm dba o zapasowe źródła zasilania sprzętu informatycznego.

Wszystkie badane IF i większość dużych badanych jednostek ma wyodrębnione specjalne strefy bezpieczeństwa, takie jak na przykład: serwerownia, archiwum przechowywania danych itp. W większości małych i ponad połowie średnich jednostek nie

wyodrębniono takich stref. Prawdopodobnie w niektórych mniejszych jednostkach istnieje problem lokalowy w tym zakresie. W firmach rodzinnych, a także w firmach o małej fluktuacji pracowników, np. biurach rachunkowych, występuje mniej sformalizowany charakter kultury organizacyjnej oparty bardziej na zaufaniu a nie na formalnych procedurach.

Większość badanych jednostek przeprowadza okresową weryfikację legalności oprogramowania zainstalowanego na komputerach, w tym IF – 100%. Tylko w co piątej małej jednostce sektora prywatnego, z wyjątkiem BRiA, podjęło taką inicjatywę.

W większości badanych jednostek opracowano dokumenty (procedury, instrukcje, szczegółowe polityk) opisujące system bezpieczeństwa danych informatycznych. Ale w mniej niż połowie jednostek nie ma procedur awaryjnych dla SIR. Tylko badane IF miały takie procedury.

Szczegółowe wyniki badań empirycznych na temat stosowania procedur organizacyjno-administracyjnych oraz zabezpieczeń fizyczno-technicznych i programowych w obszarze zapewnienia bezpieczeństwa informatycznego w jednostkach zawarto w tabeli 4.

Tabela 4. Stosowanie procedur organizacyjnych oraz zabezpieczeń technicznych i programowych w obszarze zapewnienia bezpieczeństwa informatycznego w badanych jednostkach

Pytanie	Odpowiedzi tak (dane w %)						
	JST	**IF**	**BR i A**	**FP 20**	**FP 100**	**FP >100**	**Średnia**
1. Czy w jednostce opracowano dokumenty (procedury, instrukcje, szczegółowe polityki) opisujące system bezpieczeństwa danych informatycznych?	63	100	59	35	53	87	66
2. Czy opracowano procedury awaryjne dla SIR?	54	86	59	23	41	55	53
3. Czy obowiązujące procedury/instrukcje w zakresie ochrony ZIR są aktualne, tzn. zgodne z obowiązującymi przepisami prawa i regulacjami wewnętrznymi (np. regulaminem organizacyjnym, procedurami)?	79	100	93	34	44	72	70
4. Czy dokumenty i inne zasoby informatyczne, z których korzysta Pani/Pan w swojej pracy są odpowiednio chronione przed utratą lub zniszczeniem?	72	100	83	46	61	72	72
5. Czy w jednostce w regularnych odstępach czasu tworzy się rezerwowe kopie danych?	86	100	79	36	68	87	76
6. Czy rezerwowe kopie danych przechowuje się w wydzielonych i zabezpieczonych pomieszczenia dla tego celu?	73	100	27	21	53	72	58

ciąg dalszy tab. 4

Pytanie	Odpowiedzi tak (dane w %)						
	JST	**IF**	**BR i A**	**FP 20**	**FP 100**	**FP >100**	**Średnia**
7. Czy SIR wymuszają okresową zmianę hasła przez użytkownika?	83	100	93	38	68	87	78
8. Czy w jednostce jest procedura przydzielania użytkownikom systemów uprawnień do danych, funkcji programów i komputerów?	78	100	45	21	60	83	65
9. Czy organizowane są szkolenia dla nowozatrudnionych pracowników w zakresie bezpieczeństwa danych informatycznych?	42	94	59	16	44	61	53
10. Czy w jednostce stosuje się procedury i zabezpieczenia przed pozyskaniem danych informatycznych wobec osób i firm współpracujących, np. firm sprzątających, serwisu informatycznego itd.?	61	94	31	16	38	58	50
11. Czy jednostka stosuje zapasowe źródła zasilania sprzętu informatycznego?	90	100	59	46	68	87	75
12. Czy w jednostce wyodrębniono specjalne strefy bezpieczeństwa, takie jak np.: serwerownia, archiwum przechowywania danych itp.?	69	100	10	23	41	87	55
13. Czy w jednostce przeprowadza się okresową weryfikację legalności oprogramowania zainstalowanego na komputerach?	63	100	86	23	60	72	67

Źródło: opracowanie własne.

Zakończenie

Współczesne uwarunkowania funkcjonowania jednostek gospodarczych w cyberprzestrzeni organizacyjnej, publicznej i globalnej pokazują, że z jednej strony technika informatyczna (IT) pozwala na nieograniczone możliwości rozwoju organizacyjnego i prowadzenia biznesu, a drugiej strony równocześnie wnosi do jednostki coraz to trudniejsze do zidentyfikowania wewnętrzne i zewnętrzne zagrożenia dla bezpieczeństwa informatycznego ZIR. Chociaż problemy ochrony ZIR w jednostkach są regulowane przez UoR od 1995 r., to jednak w praktyce, ze względu na ciągły rozwój IT oraz wzrost liczby i rodzajów cyberzagrożeń, zapewnienie wiarygodnej informacji finansowej oraz bezpieczeństwa ZIR w jednostce wymaga ciągłego dostosowywania systemu zarządzania bezpieczeństwem informatycznym do warunków funkcjonowania jednostki w złożonej cyberprzestrzeni.

Podstawowym celem podjętych badań empirycznych było ustalenie czy po wprowadzeniu prawie ćwierć wieku temu pierwszych zapisów w UoR w przedmiotowym zakresie badania w polskich jednostkach nadal istnieją obszary niekompetencji albo braku wiedzy, a może niekiedy ignorancji lub też złej woli do podejmowania działań w zakresie ochrony ZIR przez kierownictwo jednostek. Wyniki badań prezentują podejście kierownictwa do kształtowania środowiska wewnętrznego, komunikacji wewnętrznej i kontroli w zakresie zapewnienia ochrony ZIR, a także do różnych aspektów zarządzania ryzykiem informatycznym oraz na jakim poziomie stosuje się procedury organizacyjno-administracyjne, zabezpieczenia fizyczno-techniczne i programowe. W konsekwencji odpowiedzi ankietowe pokazały jak kierownictwo badanych podmiotów stosuje w praktyce wymogi UoR w zakresie zapewnienia wiarygodnej informacji finansowej oraz bezpieczeństwa ZIR.

Przeprowadzone badania empiryczne pozwoliły pozytywnie zweryfikować obie hipotezy postawione we wprowadzeniu opracowania. Można jednoznacznie stwierdzić, że kierownictwo, zarówno w instytucjach finansowych, jak i w jednostkach sektora finansów publicznych, stosując dodatkowe regulacje sektorowe (Rekomendacja D i H dla banków oraz Standardy kontroli zarządczej dla jednostek sektora finansów publicznych i wytyczne dotyczące zarządzania ryzykiem), ma znacznie większe doświadczenie i przywiązuje znacznie większą wagę do aspektów organizacyjnych kontroli wewnętrznej w obszarze zapewnienia bezpieczeństwa informacji i ochrony ZIR. Jednostki w tych sektorach mają opracowane szczegółowe i – co szczególnie ważne – aktualne zasady procedury i instrukcje, które są dostępne dla pracowników, a także szkolą pracowników w tym zakresie. Od wielu lat stosują określone „dobre praktyki" poprawiające bezpieczeństwo informacji oraz ZIR. Przeprowadzają one systematyczną analizę zagrożeń i szacowanie ryzyka (świadczą o tym pisemne rejestry ryzyka i identyfikacja istotnych ryzyk), a także dostosowują do wyników tej analizy rozwiązania organizacyjno-administracyjne oraz fizyczne, techniczne i programowe zabezpieczenia. Również wyniki badań uzyskane w związku z wyodrębnieniem z próby badawczej biur rachunkowych i małych firm audytorskich z jednostek w sektorze prywatnym, potwierdziły, że podmioty te lepiej niż większość jednostek z sektora prywatnego, stosują się do przepisów UoR w obszarze bezpieczeństwa ZIR. Szczególna ochrona zbiorów informacji finansowej w instytucjach finansowych, jednostkach sektora finansów publicznych oraz biurach rachunkowych i firmach audytorskim, ma także związek z publicznym charakterem ich działalności oraz odpowiedzialności za bezpieczeństwo informacji wobec klientów tych podmiotów.

Zdaniem autorki, problemy analizowane w niniejszym opracowaniu wymagają ciągłej dyskusji naukowej prowadzącej m.in. do opracowywania modeli teoretycznych (w tym także nowoczesnych systemów bezpieczeństwa informatycznego, kontroli wewnętrznej), wskazywania skutecznych metod i narzędzi kadrze kierowniczej jednostek (np. zarządzania ryzykiem, kontroli, samooceny i audytu), a także wskazywania odpowiednich inicjatyw legislacyjnych, bowiem właściwe regulacje, ich wdrożenie, a w szczególności skuteczne egzekwowanie, wpływają na zwiększenie bezpieczeństwa informatycznego jednostek.

Literatura

Andrzejewski M., Jonas K., Młodkowski P. (2004), *Zastosowanie technik komputerowych w rachunkowości: systemy dla małych i średnich przedsiębiorstw*, Oficyna Ekonomiczna, Kraków.

Barclay C. (2014), *Using Frugal Innovations to Support Cybercrime Legislations in Small Developing States: Introducing the Cyber-Legislation Development and Implementation Process Model (Cyber-Leg-DPM)*, „Information Technology for Development", 20 (2), s. 165–195.

Bartoszewicz A., Bartoszewicz S. (2016), *Rola i zadania audytu bezpieczeństwa systemów informatycznych na przykładzie jednostki sektora administracji rządowej*, „Finanse. Rynki Finansowe. Ubezpieczenia", 6(80, cz. 1), s. 269–279.

Białas A. (2007), *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa.

COSO (1994), *Internal Control – Integrated Framework*, The Committee of Sponsoring Organizations of the Treadway Commission.

COSO II (2004), *Enterprise Risk Management – Integrated Framework*, The Committee of Sponsoring Organizations of the Treadway Commission.

Dudek E. (2002a), *Dokumentacja informatycznego systemu przetwarzania danych księgowych w świetle znowelizowanej ustawy o rachunkowości*, „Zeszyty Teoretyczne Rachunkowości", 9 (65), s. 28–41.

Dudek E. (2002b), *Zasady prowadzenia komputerowych ksiąg rachunkowych w świetle znowelizowanej ustawy o rachunkowości*, „Zeszyty Teoretyczne Rachunkowości", 7 (63), s. 27–38.

Dudek E. (2002c), *Zasady polityki bezpieczeństwa systemu informatycznego rachunkowości a wymagania ustawy o rachunkowości*, „Zeszyty Teoretyczne Rachunkowości", 11 (67), s. 5–23.

Dudek E. (2003), *Zagrożenia występujące w środowisku informatycznym rachunkowości*, „Monitor rachunkowości i Finansów", 7–8.

Dudek M., Szczepankiewicz E.I. (2008), *Karta audytu wewnętrznego w jednostce sektora finansów publicznych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego", 512, Finanse. Rynki Finansowe. Ubezpieczenia, 12.

Dudek M., Szczepankiewicz E.I., Szczepankiewicz P. (2008), *Opis procedur audytu wewnętrznego w jednostce sektora finansów publicznych z wzorami dokumentów*, „Poradnik Rachunkowości Budżetowej", 7.

Dziedziczak I., Stępniewski J. (1999), *System rachunkowości wspomaganej komputerem*, SKwP, Warszawa.

Etro F. (2010), *Introducing Cloud Computing. Results from a simulation study*, „International Think-tank on Innovation and Competition", November .

Fisher R.P. (1984), *Information Systems Security*, Prentice-Hall Inc., Englewood Cliffs.

Kifner T. (1999), *Polityka bezpieczeństwa i ochrony informacji*, Helion, Gliwice.

Knapp K.J., Morris R.F, Marshall T.E., Byrd T.A. (2009), *Information security policy: An organizational-level process model*, "Computer & Security", 28 (7), s. 493.

Kshetri N. (2009), Positive Externality, *Increasing Returns, and the Rise in Cybercrimes*, „Communications of the ACM", 52 (12).

Kunz B., Tymińska A. (2014), *System informatyczny rachunkowości i jego rola w świetle ustawy o rachunkowości*, „Nauki o Finansach", 3 (20), s. 44–58.

Łapiński K., Wyżnikiewicz B. (2011), *Raport. Cloud Computing wpływ na konkurencyjność przedsiębiorstw i gospodarkę Polski*, Instytut Badań nad Gospodarką Rynkową, Warszawa.

Liderman K. (2012), *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa.

Luty Z., Biernacki M., Kasperowicz A, Mazur A. (2010), *Rachunkowość komputerowa*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław.

Mell P., Grance T. (2009), *The NIST Definition of Cloud Computing*, Ver. 15, 10.07.2009 r., http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf (dostęp z 15.05.2015).

Mitnick K., Simon W. (2002), *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons, Inc., New York.

Pałęga M., Knapiński M., Kulma W. (2014a), *Ocena systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie w świetle przeprowadzonych badań*, Oficyna Wydawnicza PTZP, Opole, s. 419–428.

Pałęga M., Knapiński M., Kulma W. (2014b), *Zarządzanie ryzykiem w systemie bezpieczeństwa informacji w przedsiębiorstwie*, „Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Technika. Informatyka, Inżynieria Bezpieczeństwa", 2, s. 223–238.

Ramin K.P., Reiman C.A. (2013), *IFRS and XBRL*, Wiley & Sons, London, s. 458–469.

Scapens R.W., Ezzamel M., Burns J., Baldvinsdottir G. (2003), *The future Direction of UK Management Accounting Practice*, Elsevier/CIMA Publications, London.

Siegel G., Sorensen J.E. (1999), *Counting More, Counting Less: The New Role of Management Accountants*, „Transformations in the Management Accounting Profession", November, 3.

Smith K.T, Smith L.M., Smith J.L. (2011), *Case Studies of Cybercrime and The Impact on Marketing Activity and Shareholder Value*, „Academy of Marketing studies Journal", 15 (2), s. 76.

Stawowski M. (1998), *Ochrona informacji w sieciach komputerowych*, Wydawnictwo ArsKom, Warszawa.

Szczepankiewicz E.I. (2016), *Audyt kontroli wewnętrznej rachunkowości w środowisku informatycznym*, Difin, Warszawa.

Szczepankiewicz E.I. (2017), *Kontrola zarządcza w jednostkach samorządu terytorialnego. Ocena i doskonalenie kontroli zarządczej w środowisku informatycznym rachunkowości*. UE i Wydawnictwo Naukowe CONTACT, Poznań.

Szczepankiewicz E., Dudek M. (2008), *Zarządzanie bezpieczeństwem informacji w polskich i zagranicznych podmiotach gospodarczych w świetle wyników badań w latach 2004–2007*, „Zeszyty Naukowe Wyższej Szkoły Handlu i Rachunkowości w Poznaniu". Gospodarka a społeczeństwo informacyjne, s. 174–185.

Szczepankiewicz E., Dudek M. (2009), *Rozwój technologii informatycznych a zagrożenia i zarządzanie bezpieczeństwem informacji w przedsiębiorstwach*, [w:] M. Grzybowski, J. Tomaszewski (red.), *Logistyka. Komunikacja, Bezpieczeństwo. Wybrane problemy*, Wydawnictwo Wyższej Szkoły Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni, Gdynia, s. 263–274.

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

Unold J. (2015), *Zarządzanie informacją w cyberprzestrzeni*, Wydawnictwo Naukowe PWN, Warszawa.

Wasilewski J. (2013), *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego", 9 (5), s. 225–234.

Wójcik J.W. (1999), *Przestępstwa komputerowe, Część 1 – Fenomen cywilizacji*, CIM, Warszawa.

Zaleska B. (2011a), *Dobór systemów komputerowych do prowadzenia ksiąg rachunkowych*, [w:] K. Winiarska (red.), *Organizacja rachunkowości*, PWE, Warszawa, s. 94–101.

Zaleska B. (2011b), *Komputerowa ewidencja operacji gospodarczych*, (w:) K. Winiarska (red.), *Organizacja rachunkowości w małych i średnich przedsiębiorstwach regionu koszalińskiego*, Wydawnictwo Uczelniane Politechniki Koszalińskiej, Koszalin, s.76–84.

Zaleska B., Dziadek K. (2013), *Nowe obowiązki w zakresie bezpieczeństwa informacyjnego jednostek realizujących zadania publiczne*, „Rozprawy i Studia Uniwersytetu Szczecińskiego", 874, s. 359 – 370.

Akty prawne i inne regulacje

Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (2013), Komisja Nadzoru Finansowego, Warszawa.

Rekomendacja H dotycząca kontroli wewnętrznej w banku (2011), Komisja Nadzoru Finansowego, Warszawa.

Komunikat nr 6 Ministra Finansów z 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem, Dz.Urz. Min.Fin. poz. 56.

Standardy kontroli zarządczej (2009), Załącznik do Komunikatu nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla jednostek sektora finansów publicznych. Dz. Urz. Min. Fin. 2009, nr 15, poz. 84.

Stanowisko Komitetu Standardów Rachunkowości z dnia 13 kwietnia 2010 r. w sprawie niektórych zasad prowadzenia ksiąg rachunkowych (2010), Załącznik do Komunikatu nr 10 Ministra Finansów z dnia 18.05.2010 r. w sprawie ogłoszenia uchwały Komitetu Standardów Rachunkowości w sprawie przyjęcia stanowiska Komitetu w sprawie niektórych zasad prowadzenia ksiąg rachunkowych. Dz. Urz. Min. Fin. 2010 r. nr 6 poz. 26).

Ustawa z 29 września 1994 roku o rachunkowości, Dz.U. 2009, nr 152, poz. 1223.

Ustawa z 29 września 1994 roku o rachunkowości, tj. Dz.U. 2016, poz. 615 ze zm.

Ustawa z dnia 10 września 2015 r. o zmianie ustawy – *Ordynacja podatkowa*, Dz.U. 2015, poz. 1649 ze zm.

Ustawa z dnia 26 września 2014 r. o zmianie ustawy o podatku dochodowym od osób fizycznych oraz niektórych innych ustaw, Dz.U. 2014, poz. 1563 ze zm.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 2015 poz. 2135 ze zm.

Ustawa z dnia 17 listopada 1964 r.– *Kodeks postępowania cywilnego*, Dz.U. 2014 poz. 101 ze zm.

Ustawa z dnia 28 listopada 2014 r. o zmianie ustawy – *Kodeks spółek handlowych oraz niektórych innych ustaw*, Dz.U. 2015 poz. 4 ze zm.

Źródła internetowe

Encyklopedia PWN (2016), https://encyklopedia.pwn.pl/ (dostęp 12.02.2016).

Raport CERT (2016), www.cert.orange.pl (dostęp 12.05.2016).

Raport KPMG (2016), *Cyberbezpieczeństwo – wyzwanie współczesnego prezesa*, https://assets.kpmg.com (dostęp 12.05.2016).

Raport PwC (2016), *W obronie cyfrowych granic czyli 5 rad, aby realnie wzmocnić ochronę firmy przed CYBER ryzykiem*, Warszawa, https://www.pwc.pl (dostęp 1.04.2016).

*Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 (*2010), Warszawa. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland _Cyber_Security_Strategy.pdf (dostęp 12.02.2012).