BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-007
Data wpłynięcia: 4.05.2023
Data akceptacji: 14.09.2023

Wojciech Kozioł

dr, Uniwersytet Ekonomiczny w Krakowie
https://orcid.org/0000-0001-7920-760X

Paweł Łojek

mgr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0003-4049-4626

Praktyka bezpieczeństwa danych w systemie rachunkowości w świetle badań empirycznych

Wprowadzenie

Z prowadzeniem działalności gospodarczej wiąże się konieczność jej dokumentacji, ewidencji i okresowego rozliczania. Do tego celu służy system rachunkowości, który ma zapewnić wiarygodne i rzetelne źródło informacji o sytuacji ekonomiczno-finansowej podmiotów. Informacje te stanowią niezwykle wrażliwy obszar funkcjonowania organizacji, dlatego zarówno w krajowych, jak i międzynarodowych regulacjach z zakresu organizacji systemu rachunkowości wiele miejsca poświęcono właśnie problematyce bezpieczeństwa danych księgowych. Czwarta rewolucja przemysłowa sprawia, że otwierają się nowe perspektywy dla prowadzenia i rozwijania działalności gospodarczej – dzięki rozwiązaniom, jakie daje cyberprzestrzeń[1]. Jak powszechnie wiadomo, główny cel prowadzenia działalności gospodarczej to maksymalizacja zysków przy minimalnym zaangażowaniu kapitału. Cyfryzacja nie omija również systemu rachunkowości organizacji. Dzieje się tak z przyczyn organizacyjnych i prawnych. Cyfryzacja usprawnia bowiem proces przetwarzania informacji w organizacji

[1] E.I. Szczepankiewicz, *Zarządzanie bezpieczeństwem zasobów informatycznych rachunkowości w polskich jednostkach – wyniki badań*, „Zeszyty Teoretyczne Rachunkowości" 2018, t. 97, nr 153, s. 115–138.

i w jej otoczeniu gospodarczym. Obowiązkiem organizacji jest rzetelne rozliczenie się nie tylko z właścicielami, ale również z instytucjami państwowymi. Wprowadzone w ostatnich latach regulacje prawne nakładają na organizacje realizację kolejnych obowiązków sprawozdawczych w formie elektronicznej. Przykładem tego jest obowiązek okresowego przesyłania dokumentów elektronicznych: sprawozdań finansowych do Krajowego Rejestru Sądowego (KRS) i deklaracji podatkowych związanych z rozliczaniem podatków: podatku od towarów i usług (VAT), podatku dochodowego od osób prawnych (CIT) i innych (np. VAT-7 w formie tzw. jednolitego pliku kontrolnego (JPK)) – czy też ubezpieczeniowych, wynikających chociażby z ustawy o systemie ubezpieczeń społecznych[2]. Dokumenty te bazują na danych księgowych, co – niezależnie od aspektów organizacyjnych – wymusza na organizacjach digitalizację systemu finansowo-księgowego.

Ostatnie dwie dekady charakteryzuje powszechność systemów cyfrowych. Z punktu widzenia ewolucji społecznej jest to stosunkowo krótki okres. Powoduje to, że w porównaniu do systemów tradycyjnych, istnieje ograniczona świadomość istniejących zagrożeń. Ponadto reakcje ludzi na cyfrowe zagrożenia nie są tak intuicyjne, jak ma to miejsce w przypadku zagrożeń dla tradycyjnych rozwiązań.

Problematyka bezpieczeństwa danych stanowi szczególnie ważną kwestię w przypadku systemu rachunkowości, którego funkcją jest przetwarzanie szerokiego zakresu danych. Dane te zbierane są w trakcie roku obrotowego w następstwie procesu ewidencji wszystkich zdarzeń wywołujących skutki gospodarcze. Następnie w procesie odpowiedniej agregacji tych danych sporządzane są sprawozdania finansowe. Sprawozdania finansowe z założenia mają być wiarygodnym i rzetelnym źródłem informacji o sytuacji ekonomicznej jednostki, które znajdują zastosowanie w procesach decyzyjnych przebiegających wewnątrz jednostki, jak i w jej otoczeniu. Poza obowiązkowymi sprawozdaniami finansowymi, dane finansowe służą również do generowania raportów i zestawień przygotowywanych na potrzeby bieżącego i strategicznego zarządzania jednostką bądź jej poszczególnymi obszarami. Jak można zauważyć, utrata dostępu do tych danych może stanowić realne zagrożenie dla działania jednostki. Problem ten jest dodatkowo potęgowany przez rosnące zapotrzebowanie na informacje pochodzące z systemu rachunkowości, m.in. z powodu wzrostu złożoności powadzenia działalności gospodarczej, jak i pojawiających się nowych tendencji do poszerzania zakresu informacji sprawozdawczej o tzw. dane niefinansowe. Są to informacje środowiskowe i społeczne, które wchodzą w zakres społecznej odpowiedzialności jednostek.

Bezpieczeństwo systemu rachunkowości stanowi istotną kwestię organizacyjną. Uzasadnia to potrzebę identyfikacji zakresu znajomości tych zagrożeń oraz świadomego przeciwdziałania im poprzez stosowanie wymaganych prawem zaleceń. Celem

[2] Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, tekst jedn. Dz.U. z 2022 r., poz. 1009.

artykułu jest zdefiniowanie rozwiązań, jakie przewiduje podstawowy akt normatywny regulujący rachunkowość podmiotów gospodarczych: ustawa z dnia 29 września 1994 r. o rachunkowości[3] (dalej: UoR), oraz inne regulacje określone prawem polskim i niektórymi postanowieniami międzynarodowymi. Przedstawione badania mają odpowiedzieć na pytanie, czy podmioty gospodarcze z wybranej próby badawczej potrafią wskazać rozwiązania, jakie nakłada UoR czy też inne regulacje prawne w omawianym obszarze. Powstaje również pytanie, czy rozwiązania te są stosowane regularnie, czy też wybiórczo. Na próbę badawczą składają się podmioty sporządzające sprawozdania w oparciu o postanowienia UoR jak również Międzynarodowych Standardów Rachunkowości (MSR) zastąpionych od 2001 r. przez Międzynarodowe Standardy Sprawozdawczości Finansowej (MSSF)[4].

W artykule postawiono następujące hipotezy badawcze:

H1: Bezpieczeństwo danych w rachunkowości, w wybranej próbie badawczej wzrosło na przestrzeni analizowanego okresu.

H2: Podmioty poszukują nowych rozwiązań, wykraczających poza postanowienia UoR.

H3: Podmioty starają się zapobiegać ryzyku utraty danych poprzez rozbudowę sieci IT.

Niniejszy artykuł wykorzystuje metody badawcze takie jak analiza i krytyka piśmiennictwa i wyników badań naukowych oraz wnioskowanie statystyczne.

Bezpieczeństwo systemu rachunkowości w świetle uregulowań krajowych i międzynarodowych

Pojęcie bezpieczeństwa

Bezpieczeństwo jest pojęciem wieloznacznym i w zależności od obszaru analizy czy dziedziny wiedzy może być rozumiane w różny sposób. Dodatkowo występuje także w połączeniu z innymi pojęciami i w ten sposób uzyskuje kolejne konteksty znaczeniowe. W efekcie istnieje wielka różnorodność w rozumieniu tego pojęcia. W sytuacji, gdy te same pojęcia są stosowane w wielu obszarach wiedzy lub są pojęciami interdyscyplinarnymi, istnieje niebezpieczeństwo niewłaściwego rozumienia znaczenia specyficznego dla odrębnej specjalności naukowej czy dziedziny wiedzy[5].

Kwestia bezpieczeństwa jest ściśle związana ze stanem analizowanego obiektu. Bezpieczeństwo danego podmiotu to obszar jego aktywności, którego treścią jest

---

[3] Ustawa z dnia 29 września 1994 r. o rachunkowości, tekst jedn. Dz.U. z 2021 r., poz. 217.

[4] P. Łojek, *Wyzwania i odpowiedzialność biegłego rewidenta przy badaniu spółek giełdowych z WIG30*, [w:] *Wyzwania rewizji finansowej*, red. K. Chłapek, S. Krajewska, P. Zieniuk, Difin, Warszawa 2020, s. 129–148.

[5] R. Klamut, *Bezpieczeństwo jako pojęcie psychologiczne*, „Zeszyty Naukowe Politechniki Rzeszowskiej. Ekonomia i Nauki Humanistyczne" 2012, z. 19, nr 4, s. 41–51.

zapewnianie możliwości przetrwania i dalszej egzystencji, a także swobody realizacji własnych interesów w niebezpiecznym środowisku, w szczególności poprzez wykorzystywanie szans, redukowanie ryzyka oraz przeciwdziałanie wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów. U podstaw rozwiązywania najistotniejszych problemów bezpieczeństwa leży niewątpliwie ocena zagrożeń[6].

Z perspektywy każdego człowieka, bezpieczeństwo to przede wszystkim jedna z jego potrzeb, która została szeroko opisana na gruncie nauk psychologicznych. Jednak system finansowo-księgowy stanowi tzw. obiekt antropogeniczny, czyli obiekt techniczny stworzony celowo przez człowieka, przeznaczony dla realizacji różnorodnych jego potrzeb. Przeciwieństwem obiektu antropogenicznego jest obiekt naturalny, wytworzony przez przyrodę. W teorii zarządzania bezpieczeństwem ważne miejsce zajmuje nurt zarządzania bezpieczeństwem obiektu antropogenicznego, określany również mianem inżynierii bezpieczeństwa obiektów antropogenicznych. Obszarem jej zainteresowania są sposoby postępowania w procesach projektowania, wykonywania i eksploatacji obiektów antropogenicznych. Sposoby te mogą mieć charakter techniczny, ekonomiczny, prawny i organizacyjny i ukierunkowane są na:

- nadawanie tym obiektom cech umożliwiających przeciwstawienie się przewidywanym zagrożeniom (generowanym w samym obiekcie, a także w jego otoczeniu), które mogą wystąpić w czasie jego tworzenia, późniejszej eksploatacji i ewentualnej likwidacji,
- zmniejszanie przewidywanych zagrożeń generowanych w obiekcie, jak i w jego otoczeniu,
- utrzymanie określonego poziomu bezpieczeństwa obiektu przy założonym stopniu ryzyka[7].

Inżynieria bezpieczeństwa obiektów antropogenicznych dotyczy określenia i ciągłego doskonalenia metod postępowania oraz znajomości wymagań i zasad bezpieczeństwa, w tym umiejętności[8]:

- identyfikacji problemów i zadań w zakresie monitorowania, procesów decyzyjnych, eksploatacji i diagnostyki ww. obiektów oraz sposobów zarządzania nimi i inżynierią eksploatacji tych urządzeń,
- opracowywania strategii zarządzania bezpieczeństwem i działań wspierających niezawodność obiektów,
- identyfikacji potrzeb otoczenia gospodarczego i realizacji innowacyjnych działań,
- identyfikacji zagrożenia bezpieczeństwa osobistego, technologii komunikacji oraz metodyki badań inżynierskich.

---

6 S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe" 2011, nr 2 (18), s. 19–39.

7 A. Baryłka, *Podstawy inżynierii bezpieczeństwa obiektów antropogenicznych*, „Inżynieria Bezpieczeństwa Obiektów Antropogenicznych" 2015, nr 1, s. 10–16.

8 *Ibidem.*

Specyfika funkcjonowania cyfrowego systemu rachunkowości

Powszechna informatyzacja procesu wymiany informacji zachodząca w ramach systemu rachunkowości powoduje, że system ten funkcjonuje w warunkach określonych przez cyberprzestrzeń. Cyberprzestrzeń można zdefiniować jako kompleksową, automatyczną, złożoną sieć, oderwaną od realnego świata, zbudowaną z wykorzystaniem infrastruktury teleinformatycznej, w której funkcjonowanie człowieka staje się możliwe, a generowane w niej informacje są podstawą istnienia i stają się dobrem najwyższej jakości. Włączenie danego obszaru funkcjonowania organizacji do cyberprzestrzeni można określić mianem cyfryzacji. Cyfryzacja to działanie z wykorzystaniem narzędzi cyfrowych, mające na celu zwiększenie produktywności dzięki wprowadzeniu innowacyjnych produktów i usług, optymalizacji procesów organizacyjnych oraz bardziej efektywnemu wykorzystaniu zasobów takich jak zasoby techniczne, kapitał ludzki czy informacja[9].

Systemy informacyjne, takie jak systemy finansowo-księgowe, mają na celu gromadzenie danych, których ilość jest niemal nieograniczona, co daje im znaczną przewagę nad rozwiązaniami tradycyjnymi. Połączenie znacznej ilości danych z odpowiednim sposobem ich analizy ma przełożenie na rzetelność, wiarygodność oraz szybkość i łatwość pozyskania informacji finansowych. Z drugiej strony z procesem informatyzacji wiążą się też wady. Systemy wymagają czasochłonnych i kosztownych procesów wdrożeniowych i dostosowawczych oraz przeciwdziałania dezaktualizacji technologii. Dodatkowym zagrożeniem dla systemu jest aktywność w sieci, co rodzi ryzyko utraty lub kradzieży danych. Ponadto proces cyfryzacji, w tym cyfryzacji księgowości, wymaga zaangażowania odpowiednio wykwalifikowanych pracowników, których kompetencje są nieustannie aktualizowane. Wskazuje się również, że zmaterializowanie się wspomnianych zagrożeń może wypaczyć proces analizy danych, prowadząc do naruszenia zasady wiernego i rzetelnego obrazu[10].

Coraz szerszy zakres ujawnianych danych wymaga jednak nowych rozwiązań w rachunkowości, dlatego w coraz większym stopniu wykorzystuje się narzędzia informatyczne, takie jak[11]:

- big data,
- hurtownie danych,
- cloud computing (przetwarzanie w chmurze),
- blockchain.

---

[9] A. Kuczyńska-Cesarz, *Selected areas of threats to the security of accounting information system*, „Inżynieria Bezpieczeństwa Obiektów Antropogenicznych" 2021, nr 3, s. 37–49.

[10] D. Qin, *Designing an Accounting Information Management System Using Big Data and Cloud Technology*, „Scientific Programming" 2022, vol. 33, https://doi.org/10.1155/2022/7931328.

[11] T. Spychała, *Rozwój rachunkowości a cyberprzestrzeń w społeczeństwie sieci*, „Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze" 2019, nr 11, s. 109–118.

Nieco inną klasyfikację zagrożeń w systemie informatycznym przedsiębiorstwa przedstawia Kamila Schneider i Karol Schneider[12]:

1. Ze względu na źródło:
   a) zagrożenia wewnętrzne, na które jednostka ma wpływ:
   – organizacyjne, wynikające z nieprawidłowej organizacji jednostki,
   – technologiczne, będące następstwem błędów technologicznych,
   b) zewnętrzne, pochodzące z otoczenia jednostki gospodarczej.
2. Ze względu na celowość działania:
   a) przypadkowe (losowe),
   b) celowe (umyślne).
3. Ze względu na rodzaj zagrożenia:
   a) dotyczące oprogramowania,
   b) dotyczące sprzętu.
4. Ze względu na wynik – zagrożenia prowadzące do:
   a) całkowitej utraty danych,
   b) kradzieży informacji (wycieku danych),
   c) ingerencji w przetwarzane dane.

Bezpieczeństwo danych w systemach finansowo-księgowych

Ochrona danych w systemach informatycznych, audyty systemów informatycznych czy też bezpieczeństwo ich danych były przedmiotem rozważań wielu autorów[13]. Publikacje te wskazały rozwiązania, jakie należy przyjąć w zakresie ochrony danych rachunkowych w jednostkach gospodarczych. Postępująca informatyzacja podmiotów gospodarczych oraz liczne czynniki zewnętrzne i wewnętrzne powodują konieczność rozszerzania dotychczas stosowanej technologii, a także poszukiwanie nowych rozwiązań. Autorzy tych badań postulują rozwój w obszarze bezpieczeństwa danych w rachunkowości poprzez aspekty organizacyjne, kontrolę wewnętrzną, a także wdrażanie instrukcji, procedur czy też innych schematów mających na celu poprawę ogółu funkcjonowania jednostki w tym aspekcie.

---

[12] K. Schneider, K. Schneider, *Zagrożenia w funkcjonowaniu jednolitego pliku kontrolnego*, „Ekonomiczne Problemy Usług" 2018, nr 2 (131), t. 1, s. 323–330.

[13] T. Ciesielczyk, J. Stępniewski, *Ochrona danych w systemach informatycznych rachunkowości*, „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 1994, nr 691: *Informatyka ekonomiczna*, s. 17–23; B. Galica, B. Tomczyk-Noga, *Atestacja systemów informatycznych rachunkowości*, „Prace Naukowe Akademii Ekonomicznej w Katowicach", 1997: *Rachunkowość w gospodarce rynkowej: nauka i praktyka. Materiały konferencyjne. Ogólnopolski Zjazd Katedr Rachunkowości, Ustroń 17–19 września 1997*, t. 1, s. 121–124; J. Madej, K. Szymczyk-Madej, *Prawne wymogi bezpieczeństwa systemów informatycznych w polskich przedsiębiorstwach według kodeksu karnego, ustawy o rachunkowości i ustawy o ochronie danych osobowych*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, nr 770, s. 89–107; K. Szymczyk-Madej, J. Madej, *Bezpieczeństwo informatycznych systemów rachunkowości*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2000, nr 553, s. 161–177.

W przepisach art. 71–76 UoR zostały wprowadzone regulacje dotyczące ochrony danych w jednostkach podlegających postanowieniom tej ustawy, określonych w art. 2. Ustawodawca wskazał, że komputerowe prowadzenie ksiąg rachunkowych powinno opierać się na:

- stosowaniu nośników danych, które są odporne na wszelkie zagrożenia,
- doborze odpowiednich środków ochrony zewnętrznej,
- tworzeniu rezerwowych kopii zbiorów danych odpowiednio zabezpieczonych na nośnikach informatycznych zapewniających trwałość zapisu przez określony ustawą czas (art. 74 ust. 2 UoR),
- zapewnieniu ochrony programów komputerowych oraz danych systemowych poprzez zastosowanie odpowiednich rozwiązań informatycznych i organizacyjnych.

Z analizy przepisów wynika, że UoR nie wskazuje wprost rozwiązań, jakie powinna przyjąć jednostka gospodarcza stosująca jej postanowienia. Zatem każdy podmiot gospodarczy powinien dokonać osądu oraz wskazać właściwe rozwiązania w omawianych kwestiach. Przykładowe rozwiązania zostały przedstawione w tabeli 1 – jako interpretacja przepisów UoR według autorów.

Tabela 1. Przykładowe rozwiązania w zakresie ochrony danych rachunkowych zgodnej z UoR

Rodzaj ochrony	Przykładowe rozwiązania
Ochrona danych w systemie	niekorzystanie z systemu przez osoby nieupoważnione lub nieuprawnione, zabezpieczenie przed nieupoważnionym wtargnięciem do pomieszczeń – odpowiednie drzwi, środki identyfikacji użytkowników uruchamiających komputery – hasła,
Ochrona systemu przed uszkodzeniem	przeglądy i bieżąca konserwacja sprzętu komputerowego, konserwacja standardowego oprogramowania, ochrona przed wirusami komputerowymi, współpraca z zewnętrznym serwisantem, która wykluczy długotrwałe przerwy w pracy systemu,
Ochrona przechowywanych zbiorów i dowodów księgowych	przekazywanie zbiorów i dowodów do archiwum, tworzenie kopii zapasowych informacji księgowych na zewnętrznych nośnikach

Źródło: opracowanie własne na podstawie art. 71–76 ustawy z dnia 29 września 1994 r. o rachunkowości, tekst jedn. Dz.U. z 2021 r., poz. 217.

Jak wspomniano, pewne minimalne wymagania dla systemów informatycznych wspomagających rachunkowość przedsiębiorstwa zostały podane w UoR. Nie określono jednak procedur pozwalających na stwierdzenie, czy wymagania te są spełnione w stosowanych systemach informatycznych. Warto podkreślić, że Stowarzyszenie Księgowych w Polsce (SKwP), będące największą organizacją zawodową w obszarze

rachunkowości, prowadzi aktywność polegającą na weryfikacji produktów informatycznych wspierających procesy finansowo-księgowe w organizacjach. Lista rekomendowanych programów jest dostępna na stronie internetowej SKwP[14].

Ochrona danych w systemie polega głównie na zabezpieczeniu wszelkich informatycznych systemów oraz pomieszczeń przed osobami nieuprawnionymi. Najprostszą formą ochrony jest zastosowanie haseł zabezpieczających oraz odpowiednie wyposażenie pomieszczeń i budynków w drzwi posiadające funkcję zabezpieczenia systemów informatycznych. Stosowanie odpowiednich haseł zostało wypracowane jako jedna z metod zabezpieczeń przez praktyki rynkowe, a – co ciekawe – nie przez przepisy o ochronie danych osobowych (RODO)[15].

Każde przedsiębiorstwo powinno przeprowadzić analizę ryzyka, która rozpoznaje i wskazuje potencjalne zagrożenia. Należy wśród nich uwzględnić również zasady udzielania pracownikom dostępu do zasobów informatycznych jednostki gospodarczej[16]. Ciągły rozwój systemów informatycznych oraz nowe technologie wymuszają poszukiwanie coraz to nowych systemów, w których można przechowywać dane. W początkowym etapie informatyzacji były to dyskietki, następnie nośniki CD/DVD, pamięci masowe, a obecnie – archiwizacja danych w chmurze[17].

Metodyka badań własnych i prezentacja wyników

Zgodnie z postanowieniami art. 10 ust. 1 UoR w zakresie stosowania polityki rachunkowości podmioty gospodarcze powinny określić metody ochrony danych oraz wszelkich zbiorów, dowodów księgowych oraz tych stanowiących podstawy zapisów księgowych. Zaproszenie do udziału w badaniach zostało kierowane do podmiotów współpracujących z kilkoma biurami rachunkowymi oraz autorami artykułu. Z uwagi na cel badań, były to jednostki zobowiązane do stosowania prawa bilansowego (UoR lub MSR/MSSF). Chęć udziału zgłosiła zdecydowana większość z nich. W efekcie powstała próba badawcza licząca 379 podmiotów gospodarczych – przede wszystkim

[14] *Rekomendacje dla programów księgowych*, Stowarzyszenie Księgowych w Polsce, https://skwp.pl/o-skwp/uslugi [dostęp: 28.04.2023].

[15] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (2016), Dz.U. UE L 119; zob. R. Stępniewski, *Polityka haseł w firmie*, Polityka Bezpieczeństwa, 27.06.2019, https://www.politykabezpieczenstwa.pl/pl/a/polityka-hasel-w-firmie [dostęp: 28.04.2023].

[16] M. Błażejowska, *Dostosowanie funkcjonowania spółdzielni socjalnych do RODO*, „Przedsiębiorczość i Zarządzanie" 2018, t. 19, z. 4, cz. 2: *Szanse i zagrożenia dla gospodarki europejskiej XXI wieku*, s. 39–51; M. Goddard, *The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact*, „International Journal of Market Research" 2017, vol. 59, nr 6, s. 703–705.

[17] P. Margol, P. Dymora, M. Mazurek, *Strategie archiwizacji i odtwarzania baz danych*, „Zeszyty Naukowe Politechniki Rzeszowskiej. Elektrotechnika" 2017, z. 36, nr 3, s. 31–41.

stosujących postanowienia UoR w zakresie sporządzania sprawozdań finansowych (jedynie nieliczne podmioty obserwowane w latach 2019–2020 stosują MSR/MSSF) (tabela 2).

Tabela 2. Liczba podmiotów stosujących wybrane postanowienia prawa bilansowego w latach 2016–2022

Rok obserwacji	Sprawozdawczość UoR/MSR	Liczba obserwacji w danym roku
2016	100% UoR	27
2017	100% UoR	37
2018	100% UoR	21
2019	85% UoR 15% MSR	125
2020	95% UoR 5% MSR	137
2021	100% UoR	18
2022	100% UoR	14
suma		379

Źródło: opracowanie własne.

Zgodnie z hipotezami badawczymi zawartymi we wstępie niniejszego artykułu postawiono następujące pytania badawcze:

P1: Czy w latach 2016–2022 podmioty w próbie badawczej wdrażały nowe rozwiązania w zakresie bezpieczeństwa danych?

P2: Jakie nowe technologie zostały wdrożone w celu poprawy bezpieczeństwa danych wśród uczestników próby badawczej będących przedmiotem obserwacji w kolejnym roku?

P3: Czy podmioty starają się wdrażać nowsze technologie w celu zabezpieczenia zbiorów danych?

P4: Czy podmioty dokonują inwestycji w infrastrukturę sieci IT, aby zapobiegać ryzyku utraty danych?

P5: Jak duże nakłady finansowe poniesiono w celu ograniczania ryzyka utraty danych?

P6: Czy pracownicy działu finansowo-księgowego znają postanowienia UoR w zakresie ochrony danych księgowych oraz ich zbiorów?

Nowe technologie były i są przedmiotem badań wielu autorów[18]. Wszyscy zgodnie dochodzą do wniosku, że cyberbezpieczeństwo jest niezwykle ważnym elementem

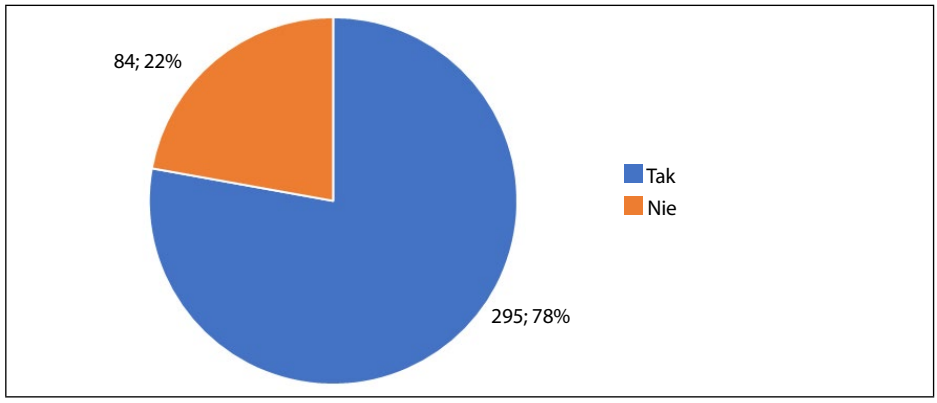
[18] T. Bąk, B. Łukaszewski, *Cyfrowe zagrożenia dla bezpieczeństwa wewnętrznego. Nowe subkultury sieciowe, wirtualna rzeczywistość, sztuczna inteligencja*, „Współczesne Problemy Zarządzania" 2020, t. 8, nr 1, s. 97–109; P. Domżał, A. Supel, P. Przybylski, *Nowoczesna technologia a wzrost cyberbezpieczeństwa – analiza zależności*, „Społeczeństwo, Kultura, Wartości. Studium społeczne" 2023, R. XIV, nr 23, s. 91–96; K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1 (17), s. 15–28.

funkcjonowania każdej jednostki gospodarczej. Poszukiwanie oraz wdrażanie nowych rozwiązań powinno wiązać się z ich doskonaleniem w celu poprawy dotychczas funkcjonujących możliwości.

Niezwykle rzadkim zjawiskiem jest dziś brak posiadania jakichkolwiek zabezpieczeń przez funkcjonujące podmioty gospodarcze. Niekiedy właściciele firm decydują się również na zakup ubezpieczeń od włamań, ataków hakerskich oraz innych powiązanych zagrożeń.

Wydawać by się mogło, że w dobie postępującej cyfryzacji dbanie oraz rozwój dotychczas funkcjonującej infrastruktury IT w zakresie bezpieczeństwa danych księgowych powinno być kwestią priorytetową. Wykres nr 1 przedstawia liczbę podmiotów oraz ich udział procentowy w omawianym zakresie.

Wykres 1. Wdrożenie nowych rozwiązań w zakresie bezpieczeństwa danych księgowych w latach 2016–2022 w analizowanej próbie badawczej

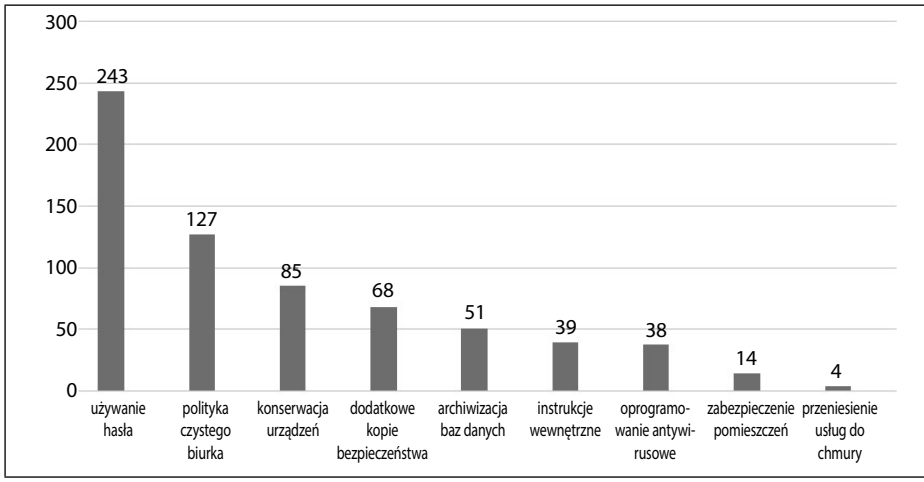


Źródło: opracowanie własne.

Przeprowadzone obserwacje wskazują, że w latach 2016–2022 w dobranej próbie badawczej 78% podmiotów dążyło do poszukiwania i wdrażania nowych rozwiązań w zakresie bezpieczeństwa danych księgowych. Niepokoić może fakt, że prawie co czwarte z badanych przedsiębiorstw w ciągu 7 lat nie dokonało żadnych uprawnień w tym obszarze. Jak wspomniano, trudno obecnie znaleźć podmiot, który nie posiada żadnych zabezpieczeń w obrębie cyberbezpieczeństwa. Można domniemywać, że takie zachowanie właścicieli i zarządzających firmami w analizowanej próbie badawczej wynika z niskiego poziomu świadomości potencjalnych zagrożeń.

Wśród podmiotów, które wdrożyły nowe technologie, postawiono pytanie, jakie konkretnie były to rozwiązania oraz którego obszaru dotyczyły. Podkreślić należy, że wybór ten nie był ograniczony do jednej możliwości, a co za tym idzie – występowały sytuacje (dość liczne) wskazań na kilka przyjętych rozwiązań.

Wykres 2. Wyszczególnienie nowych technologii wdrożonych w celu poprawy bezpieczeństwa danych w analizowanej próbie badawczej



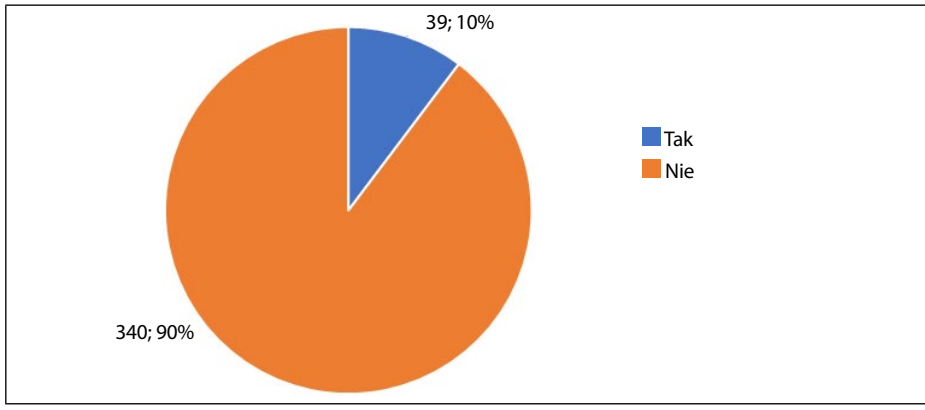
Źródło: opracowanie własne.

Jak można zaobserwować na wykresie 2, najwięcej wskazań dotyczyło używania hasła (lub wdrożenia tego rozwiązania), znaczna liczba odpowiedzi wskazywała też na wprowadzenie „polityki czystego biurka". Taki stan rzeczy może tłumaczyć obowiązywanie w Polsce od 25 maja 2018 r. rozporządzenia o ochronie danych osobowych (RODO) – obydwa ze wspomnianych powyżej rozwiązań są obligatoryjne od momentu wejścia w życie tego rozporządzenia.

Najmniej wskazań dotyczyło przeniesienia usług do tzw. chmury. Polega ono na migracji baz danych oraz całej infrastruktury na zewnątrz, co z kolei przenosi na dostawcę takich usług odpowiedzialność za wykonywanie kopii baz danych czy też innych nośników informatycznych. Jak pokazuje praktyka gospodarcza, rozwiązanie to jest dość drogie w dłuższej perspektywie, ale dla podmiotów rozpoczynających działalność może być korzystne ze względu na brak konieczności posiadania własnej, często rozbudowanej infrastruktury IT.

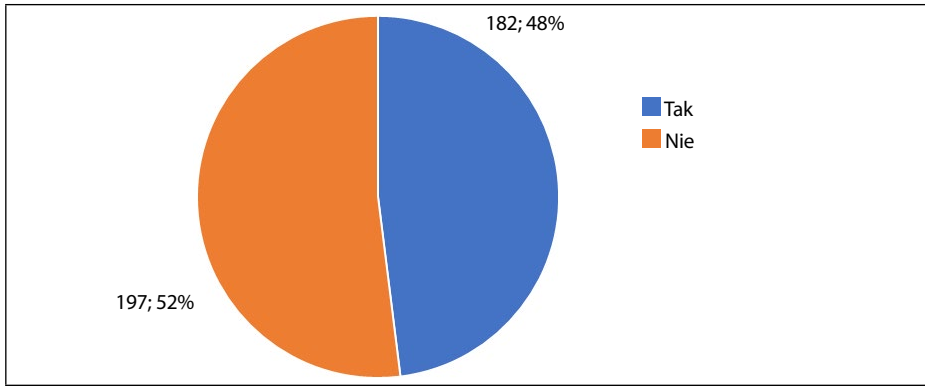
Kolejno postawiono pytanie, czy podmioty starają się wdrażać nowsze technologie w celu zabezpieczenia zbiorów danych. Co ciekawe, odpowiedź aż 340 uczestników badania, co stanowi 90% próby badawczej, można zakwalifikować jako pozytywną (wykres 3). Zjawisko to można rozpatrywać jako intrygujące: w dobie niepewności i gwałtownych wydarzeń mających miejsce na świecie (COVID-19, wojna w Ukrainie, inflacja oraz inne czynniki) podmioty starają się dążyć do zapewnienia sobie jeszcze wyższego poziomu bezpieczeństwa i do ograniczenia ryzyka utraty danych.

Wykres 3. Poszukiwanie nowych rozwiązań w zakresie poprawy bezpieczeństwa danych przez podmioty w analizowanej próbie badawczej



Źródło: opracowanie własne.

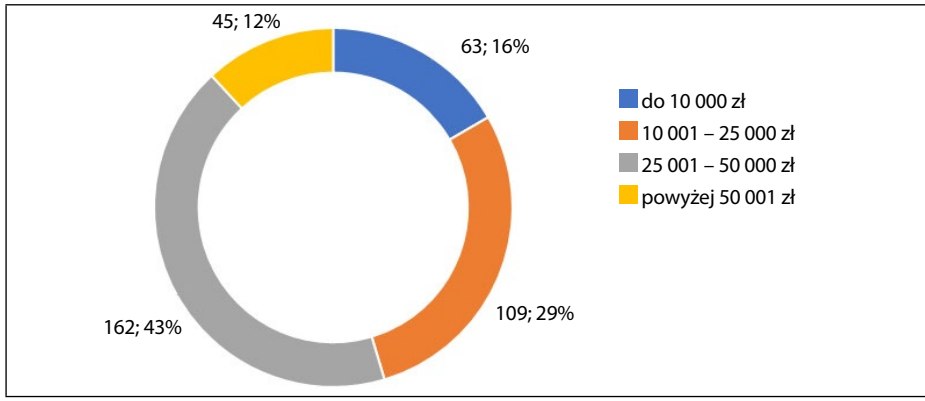
Wykres 4. Dokonywanie inwestycji w celu ograniczania ryzyka utraty danych wśród podmiotów w próbie badawczej



Źródło: opracowanie własne.

Spośród podmiotów, które udzieliły pozytywnej odpowiedzi na poprzednie pytanie, można wyszczególnić 182 jednostki, które ponadto ciągle inwestują nowe środki w rozwój infrastruktury IT związanej z poprawą zabezpieczeń zbiorów danych księgowych (wykres 4). Pozostałe 197 jednostek, co stanowi 52% podmiotów, wskazuje, że będzie bazować na rozwiązaniach, które już zostały wypracowane przez praktykę gospodarczą oraz nie są kosztowne. Obserwacji poddano również roczny poziom przewidywanych nakładów na inwestycje ograniczające ryzyko utraty danych (wykres 5).

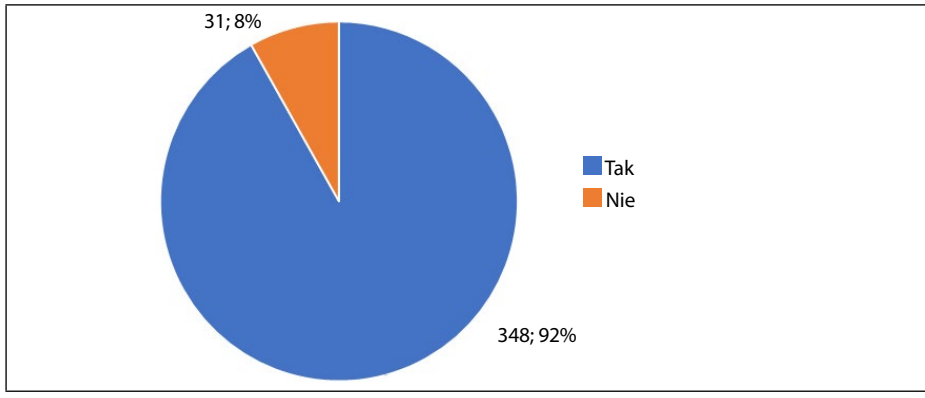
Wykres 5. Roczne nakłady finansowe na ograniczanie ryzyka utraty danych



Źródło: opracowanie własne.

Zgodnie z danymi przedstawionymi na wykresie 5, aż 43% podmiotów planujących nakłady pieniężne na poprawę bezpieczeństwa infrastruktury IT oraz ograniczanie ryzyka planuje rocznie przeznaczyć na te cele kwotę w przedziale 25 001 – 50 000 złotych. W analizowanej próbie badawczej znajdują się również podmioty (16% wszystkich obserwacji), które planują w ujęciu rocznym wygospodarować na te cele zaledwie kwotę poniżej 10 000 złotych. Zdaniem autorów artykułu kwota około 833 złote miesięcznie nie stanowi znaczącego obciążenia, patrząc przez pryzmat potencjalnych zagrożeń oraz konsekwencji wynikających z różnych aktów prawnych, szczególnie jeżeli podmiot planuje działanie w dłuższej perspektywie czasowej.

Wykres 6. Znajomość oraz świadomość stosowania rozwiązań przewidzianych w UoR w zakresie ochrony zbiorów księgowych



Źródło: opracowanie własne.

Pracownikom działów finansowo-księgowych zadano także pytanie o ich świadomość oraz umiejętność stosowania postanowień zawartych w UoR dotyczących ochrony danych zbiorów księgowych. Pozytywną odpowiedź można stwierdzić w przypadku 348 wskazań, co stanowi 92% obserwacji. Nominalnie to wysoki wynik, jednak pewnym zaskoczeniem jest fakt, że prawie co dziesiąty pracownik działu finansowo-księgowego nie zna zapisów UoR z zakresu zabezpieczenia danych księgowych, pomimo że jest to podstawowy akt normatywny regulujący prawo bilansowe w Polsce.

Podsumowanie

Problematyka zarządzania bezpieczeństwem danych, ze szczególnym uwzględnieniem danych o charakterze finansowo-księgowym, jest często podejmowanym tematem badawczym, co pozwala na bieżącą identyfikację nowo pojawiających się problemów. W efekcie liczne opracowania teoretyczne mogą być pomocne dla podniesienia poziomu bezpieczeństwa danych w organizacji.

Przeprowadzone badania wskazują, że wśród analizowanej próby badawczej stan infrastruktury IT w zakresie bezpieczeństwa oraz ochrony zbiorów księgowych znacząco się poprawił w latach 2016–2022. Po części zidentyfikowany wzrost zainteresowania kwestiami bezpieczeństwa danych księgowych był skutkiem wprowadzonego do obiegu prawnego w 2018 r. RODO. Rozporządzenie to zobowiązało wiele firm do systemowego podejścia do kwestii bezpieczeństwa danych, czego pośrednim efektem jest wzrost świadomości istnienia zagrożeń cyfrowych. Równie pozytywnie należy ocenić fakt, że mimo licznych zagrożeń, wiele podmiotów ciągle poszukuje nowych rozwiązań z zakresu bezpieczeństwa danych. Wzrost inflacji, pandemia, głębokie zmiany prawne w obszarze podatków, a w ostatnim z badanych lat – wybuch wojny, choć prowadzą do wyższego poziomu ryzyka towarzyszącego działalności gospodarczej, to jednak nie zniechęcają zarządzających do inwestycji i alokowania środków w obszar bezpieczeństwa.

Kontrowersyjną kwestią praktyczną jest przenoszenie danych do tzw. chmury, czyli środowisk wirtualnych. Z jednej strony rozwiązanie to ma swoje zalety, takie jak przeniesienie odpowiedzialności za infrastrukturę IT na zewnętrznego dostawcę, co ogranicza koszty w początkowej fazie działalności gospodarczej, z drugiej jednak – rozwiązanie to jest dość drogie jak na możliwości przedsiębiorców i realia ciągle zmieniającego się otoczenia gospodarczego.

Pomimo rosnącego dorobku nauki w tym obszarze, jak i jednoznacznie sformułowanych wymagań prawnych, część podmiotów nie wykazuje zainteresowania sprawami bezpieczeństwa danych. W praktyce gospodarczej nadal występują zarządzający przekonani o wystarczającym zabezpieczeniu zbiorów kierowanego

podmiotu. Takie przekonanie nie musi być zgodne z prawdą, a jego podstawą jest często brak wiedzy z zakresu bezpieczeństwa danych i niedostateczna świadomość istniejących zagrożeń.

Bibliografia

Baryłka A., *Podstawy inżynierii bezpieczeństwa obiektów antropogenicznych*, „Inżynieria Bezpieczeństwa Obiektów Antropogenicznych" 2015, nr 1, s. 10–16.

Bąk T., Łukaszewski B., *Cyfrowe zagrożenia dla bezpieczeństwa wewnętrznego. Nowe subkultury sieciowe, wirtualna rzeczywistość, sztuczna inteligencja*, „Współczesne Problemy Zarządzania" 2020, t. 8, nr 1, s. 97–109.

Błażejowska M., *Dostosowanie funkcjonowania spółdzielni socjalnych do RODO*, „Przedsiębiorczość i Zarządzanie" 2018, t. 19, z. 4, cz. 2: *Szanse i zagrożenia dla gospodarki europejskiej XXI wieku*, s. 39–51.

Ciesielczyk T., Stępniewski J., *Ochrona danych w systemach informatycznych rachunkowości*, „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 1994, nr 691: *Informatyka ekonomiczna*, s. 17–23.

Domżał P., Supel A., Przybylski P., *Nowoczesna technologia a wzrost cyberbezpieczeństwa – analiza zależności*, „Społeczeństwo, Kultura, Wartości. Studium społeczne" 2023, R. XIV, nr 23, s. 91–96.

Galica B., Tomczyk-Noga B., *Atestacja systemów informatycznych rachunkowości*, „Prace Naukowe Akademii Ekonomicznej w Katowicach", 1997: *Rachunkowość w gospodarce rynkowej: nauka i praktyka. Materiały konferencyjne. Ogólnopolski Zjazd Katedr Rachunkowości, Ustroń 17–19 września 1997*, t. 1, s. 121–124.

Goddard M., *The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact*, „International Journal of Market Research" 2017, vol. 59, nr 6, s. 703–705.

Klamut R., *Bezpieczeństwo jako pojęcie psychologiczne*, „Zeszyty Naukowe Politechniki Rzeszowskiej. Ekonomia i Nauki Humanistyczne" 2012, z. 19, nr 4, s. 41–51.

Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe" 2011, nr 2 (18), s. 19–39.

Kuczyńska-Cesarz A., *Selected areas of threats to the security of accounting information system*, „Inżynieria Bezpieczeństwa Obiektów Antropogenicznych" 2021, nr 3, s. 37–49.

Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1 (17), s. 15–28.

Łojek P., *Wyzwania i odpowiedzialność biegłego rewidenta przy badaniu spółek giełdowych z WIG30*, [w:] *Wyzwania rewizji finansowej*, red. K. Chłapek, S. Krajewska, P. Zieniuk, Difin, Warszawa 2020.

Madej J., Szymczyk-Madej K., *Prawne wymogi bezpieczeństwa systemów informatycznych w polskich przedsiębiorstwach według kodeksu karnego, ustawy o rachunkowości i ustawy o ochronie danych osobowych*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, nr 770, s. 89–107.

Margol P., Dymora P., Mazurek M., *Strategie archiwizacji i odtwarzania baz danych*, „Zeszyty Naukowe Politechniki Rzeszowskiej. Elektrotechnika" 2017, z. 36, nr 3, s. 31–41.

Qin D., *Designing an Accounting Information Management System Using Big Data and Cloud Technology*, „Scientific Programming" 2022, vol. 33, https://doi.org/10.1155/2022/7931328.

Rekomendacje dla programów księgowych, Stowarzyszenie Księgowych w Polsce, https://skwp.pl/o-skwp/uslugi [dostęp: 28.04.2023].

Schneider K., Schneider K., *Zagrożenia w funkcjonowaniu jednolitego pliku kontrolnego*, „Ekonomiczne Problemy Usług" 2018, nr 2 (131), t. 1, s. 323–330.

Spychała T., *Rozwój rachunkowości a cyberprzestrzeń w społeczeństwie sieci*, „Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze" 2019, nr 11, s. 109–118.

Stępniewski R., *Polityka haseł w firmie*, Polityka Bezpieczeństwa, 27.06.2019, https://www.politykabezpieczenstwa.pl/pl/a/polityka-hasel-w-firmie [dostęp: 28.04.2023].

Szczepankiewicz E.I., *Zarządzanie bezpieczeństwem zasobów informatycznych rachunkowości w polskich jednostkach – wyniki badań*, „Zeszyty Teoretyczne Rachunkowości" 2018, t. 97, nr 153, s. 115–138.

Szymczyk-Madej K., Madej J., *Bezpieczeństwo informatycznych systemów rachunkowości*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2000, nr 553, s. 161–177.

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (2016), Dz.U. UE L 119.

Ustawa z dnia 29 września 1994 r. o rachunkowości, tekst jedn. Dz.U. z 2021 r., poz. 217.

Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, tekst jedn. Dz.U. z 2022 r., poz. 1009.

Praktyka bezpieczeństwa danych w systemie rachunkowości w świetle badań empirycznych
Streszczenie

Zmieniające się otoczenie gospodarcze podmiotów prowadzących działalność wymusza na ich właścicielach oraz osobach zarządzających ciągłe dbanie o bezpieczeństwo danych. O ile przepisy prawa bilansowego nie zmieniły się znacząco od momentu ich pierwotnego wprowadzenia do stosowania (w 1994 r.), to praktyka gospodarcza wypracowała różne metody mające na celu ochronę zbioru danych księgowych.

Niniejszy artykuł składa się z części teoretycznej oraz empirycznej, a jego głównym celem jest prezentacja badań przeprowadzonych wśród wybranych podmiotów gospodarczych w zakresie tego, jak w praktyce stosują one postanowienia ustawy o rachunkowości dotyczące ochrony danych księgowych.

Wykorzystano metody badawcze takie jak analiza i krytyka piśmiennictwa i wyników badań naukowych oraz wnioskowanie statystyczne.

Słowa kluczowe: ochrona danych księgowych, poprawa bezpieczeństwa, znajomość rozwiązań dotyczących bezpieczeństwa

Data security practice in the accounting system in the light of empirical research
Abstract

The changing economic environment of business entities forces owners and managers to constantly care about data security. While the provisions of the accounting law have not

changed significantly since their initial implementation (in 1994), economic practice has developed various methods to protect the set of accounting data.

This article consists of a theoretical and an empirical part, and its main goal is to present research conducted among selected business entities in terms of how they apply the provisions of data protection of the Act on Accounting in practice.

Research methods such as analysis and criticism of literature and research results, and statistical inference were used.

Keywords: protection of accounting data, improvement of security, knowledge of security solutions