5. POLITYKA RACHUNKOWOŚCI W ZAKRESIE OCHRONY ZASOBÓW INFORMATYCZNYCH RACHUNKOWOŚCI

https://doi.org/10.18559/978-83-8211-219-1/5

Elżbieta Izabela Szczepankiewicz
Uniwersytet Ekonomiczny w Poznaniu
elzbieta.szczepankiewicz@ue.poznan.pl

Accounting policy for the protection of accounting IT resources

Abstract

The chapter outlines units obligations for the protection of accounting information resources, which result from the regulations of the Accounting Law. For computer accounting it is essential to assure an efficient protection from illegal and uncontrolled modification as well as the introduction or the removal of accounting data. The purpose of the chapter is to present the rules for the protection of data, computer software and hardware. This chapter discusses the accounting policy for the protection of accounting information resources.

Keywords: accounting policy, accounting IT resources, accounting IT system, IT environment, protection of accounting information resources.

Wprowadzenie

Wiele badań literaturowych z ostatnich lat potwierdziło, że jednym z najważniejszych czynników sprawnego zarządzania działalnością w obecnych warunkach gospodarowania jest szybkość i niezawodność pozyskiwania, gromadzenia, przetwarzania, analizy i przesyłania informacji (Dudek i Szczepankiewicz, 2009). Wiąże się to ciągłym inwestowaniem w nowe rozwiązania informatyczne, które zapewnią efektywne wspomaganie zarządzania działalnością jednostki. Stosowanie systemów informatycznych wymaga, aby na bieżąco identyfikować zagrożenia w zakresie bezpieczeństwa zasobów informatycznych. Potwierdzają to coroczne raporty na temat bezpieczeństwa informacji w jednostkach sporządzane przez różne specjalistyczne podmioty, takie jak: CERT, Ernst & Young, Deloitte, G DATA, CSI, FBI, Kaspersky oraz wiele innych.

Sugerowane cytowanie:
Szczepankiewicz, E. I. (2024). Polityka rachunkowości w zakresie ochrony zasobów informatycznych rachunkowości. W: M. Remlein i M. Masztalerz (red.), *Polityka rachunkowości w kształtowaniu obrazu jednostki gospodarczej* (s. 75–90). Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu. https://doi.org/10.18559/978-83-8211-219-1/5

Ta książka jest udostępniana na licencji Creative Commons – Uznanie autorstwa-Użycie niekomercyjne-Bez utworów zależnych 4.0 Międzynarodowe

Prezentowane przez te podmioty statystyki wskazują, że od wielu lat najbardziej znaczącym zagrożeniem w zakresie bezpieczeństwa zasobów informatycznych w jednostkach jest możliwość uszkodzenia lub zniszczenia komputerowych zbiorów danych, systemów informatycznych i sprzętu komputerowego. Zagrożenia dla zasobów informatycznych mogą wynikać zarówno z czynników losowych, błędów ludzkich, jak i celowego działania ludzi wewnątrz lub z zewnątrz jednostki. Raporty te wskazują również, że w ostatnich latach znacznie zwiększyło się ryzyko niszczenia danych przez hackerów, a nawet pozyskiwania danych przez konkurencję.

Zasoby informatyczne rachunkowości (komputerowe zbiory danych, systemy informatyczne, sprzęt komputerowy) można różnicować pod względem wartości. W obecnych czasach można stwierdzić, że zbiory danych zarówno finansowych, jak i niefinansowych, które są gromadzone w jednostce, mogą stanowić najcenniejszy element jej zasobów informatycznych. Uzasadnić można to tym, że komputer czy nośnik danych, który został zniszczony lub ukradziony, przy niezbyt wysokim koszcie nabycia można zastąpić innym. Uszkodzone oprogramowanie można ponownie zainstalować. Natomiast odtworzenie zniszczonych danych, np. z kilku miesięcy czy nawet lat, w przypadku braku albo niewłaściwie utworzonych rezerwowych kopiach danych, może być niezwykle pracochłonne i kosztowne. W konsekwencji straty jednostki o charakterze finansowym, prawnym czy wizerunkowym mogą być bardzo duże, a niekiedy nieodwracalne i mogą prowadzić do zamknięcia działalności.

Należy wspomnieć, że już ponad dwie dekady temu szybki rozwój polskiego rynku rozwiązań informatycznych dla rachunkowości oraz identyfikowanie w jednostkach coraz większej liczby nowych rodzajów ryzyka zagrażających zasobom informatycznym spowodował, że problemy bezpieczeństwa danych, ksiąg rachunkowych oraz systemów informatycznych rachunkowości stały się ważnym przedmiotem regulacji prawnych. Już w 2000 r. w znowelizowanej ustawie o rachunkowości (dalej UoR) (Ustawa, 2023) znacznie rozszerzono zakres podstawowych wymagań w zakresie ochrony tych zasobów w jednostkach(Ustawa, 2000). Wówczas formalnie zobowiązano kierowników jednostek do przyjęcia odpowiednich rozwiązań w tym zakresie i opisania ich w polityce rachunkowości.

W niniejszym rozdziale omówiono obecne wymagania UoR dotyczące systemu ochrony danych, ksiąg rachunkowych i systemów informatycznych wykorzystywanych w rachunkowości. W aspekcie regulacji prawnych wskazano najczęściej stosowane obecnie rozwiązania fizyczno-techniczne, organizacyjno-administracyjne i programowe, które przyczyniają się do zwiększenia bezpieczeństwa zasobów informatycznych rachunkowości w jednostkach. Zaprezentowano również przykładowy minimalny zakres regulacji wewnętrznych o ochronie zasobów informatycznych rachunkowości, które powinny się znaleźć w polityce rachunkowości.

5.1. Zapewnienie podstawowych środków ochrony zasobów

Należy podkreślić, że obowiązujące przepisy zawarte w UoR (Ustawa, 1994) w zakresie zasad prowadzenia ksiąg rachunkowych przy użyciu komputera oraz zasad zapewnienia bezpieczeństwa danych, ksiąg rachunkowych i systemów informatycznych rachunkowości dotyczą w takim samym zakresie każdej jednostki, która jest zobowiązana do prowadzenia ksiąg rachunkowych według UoR, niezależnie od jej wielkości, formy prawnej, przynależności do sektora czy branży. Jednocześnie należy zwrócić uwagę, że przepisy tej ustawy w zakresie bezpieczeństwa zasobów informatycznych mają jednak charakter bardzo ogólny i wyznaczają jedynie minimalne wymagania wobec jednostek gospodarczych. W ten sposób ustawodawca, poprzez zapisy o charakterze ogólnym w ustawie, wychodzi naprzeciw stosowaniu aktualnych zdobyczy informatyki i pozwala na bieżące dostosowywanie systemu ochrony zasobów informatycznych rachunkowości do specyficznych potrzeb jednostek w ciągle zmieniających się warunkach ich funkcjonowania.

Obecnie najważniejsze ogólne wymagania dotyczące prowadzenia ksiąg rachunkowych oraz ochrony danych w systemach informatycznych rachunkowości zawarto w art. 10, 13, 21, 23, 24, 71 i 72 UoR. Natomiast szczególne wymagania co do trwałości zapisu danych oraz przechowywania ksiąg rachunkowych w formie zbiorów na nośnikach komputerowych zawarto w art. 72 UoR.

Należy zwrócić szczególną uwagę na zapisy art. 71 ust. 2 UoR. W myśl tego artykułu ochrona zasobów informatycznych przy prowadzeniu ksiąg rachunkowych w systemach powinna polegać co najmniej na (Dudek, 2002b; Szczepankiewicz, 2012):

- stosowaniu w jednostce odpornych na zagrożenia nośników danych;
- systematycznym tworzeniu rezerwowych kopii zbiorów danych zapisanych na nośnikach komputerowych, które zapewniają trwałość zapisu informacji systemu rachunkowości przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych, czyli przez pięć lat;
- zapewnieniu ochrony danych, ksiąg rachunkowych i systemów informatycznych rachunkowości poprzez stosowanie odpowiednich rozwiązań programowych i organizacyjnych chroniących przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem.

W przepisach UoR określono również warunki przechowywania i ochrony dokumentacji rachunkowości niezależnie od postaci, w jakiej występują, czyli jako dane na nośnikach komputerowych lub wydruk na papierze. Ochronie w każdej postaci podlegają (Dudek, 2002a):

- księgi rachunkowe,
- dowody księgowe,
- dokumenty inwentaryzacyjne,
- sprawozdania finansowe,
- dokumentacja opisująca zasady (polityka) rachunkowości, w tym wykaz ksiąg rachunkowych i dokumentacja ewidencyjna systemów informatycznych rachunkowości dopuszczonych do eksploatacji.

W myśl zapisów art. 71 i 72 UoR informatyczne zbiory danych księgowych oraz dokumentację należy przechowywać w należyty sposób i chronić przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem. Zgodnie z art. 73 ustawy dokumentację odpowiednio oznaczoną przechowuje się w jednostce, w oryginalnej postaci, w ustalonym porządku dostosowanym do sposobu prowadzenia ksiąg rachunkowych, w podziale na okresy sprawozdawcze, w sposób pozwalający na ich łatwe odszukanie oraz przez okres określony w art. 74 UoR.

5.2. Rozwiązania fizyczno-techniczne, organizacyjno-administracyjne i programowe w zakresie ochrony zasobów informatycznych rachunkowości

Źródłami zagrożeń dla zasobów informatycznych rachunkowości mogą być różne elementy środowiska informatycznego. Może to być sieć komputerowa lub inne elementy techniczno-programowe systemu informatycznego rachunkowości (m.in. sprzęt komputerowy, wykorzystana technologia, oprogramowanie, zbiory danych), jak również personel księgowy i informatyczny, sposób organizacji pracy i kontroli, a także otoczenie zewnętrzne (Szczepankiewicz, 2014).

Do podstawowych zasobów informatycznych rachunkowości podlegających ochronie należą (Szczepankiewicz, 2019):

- sprzęt komputerowy, tj. komputery, serwery, monitory, drukarki, modemy, skanery;
- oprogramowanie systemowe, w tym: system operacyjny dla komputera, system zarządzania bazą danych, narzędzia systemowe, programy diagnostyczne;
- oprogramowanie użytkowe uniwersalne, np. arkusze kalkulacyjne, edytory tekstów;
- oprogramowanie specjalne, czyli aplikacje użytkowe rachunkowości, w tym podsystemy dziedzinowe rachunkowości: system finansowo-księgowy, system kadrowo-płacowy, system ewidencji magazynowej, rejestry VAT, system sprzedaży, system ewidencji środków trwałych i inne;

- zbiory (bazy) danych, w tym kopie bezpieczeństwa;
- elektroniczne nośniki danych;
- dokumentacja projektowa rozwiązań informatycznych, w tym systemu informatycznego rachunkowości;
- dokumentacja ewidencyjna systemu informatycznego rachunkowości;
- dokumentacja dla użytkowników poszczególnych podsystemów informatycznych rachunkowości;
- systemy zasilania, chłodzenia, klimatyzacji, ochrony przeciw pożarowej;
- sieci teletransmisyjne i centra administracyjne systemu;
- systemy ochrony dostępu fizycznego do zasobów informatycznych.

Zatem w jednostkach bardzo ważne jest stosowanie podstawowych zabezpieczeń fizyczno-technicznych pomieszczeń, a w szczególności właściwa konstrukcja i zabezpieczenia budynku, sal operacyjnych i serwerowni, sprawna instalacja klimatyzacyjna i elektryczna, środki ochrony przeciwpożarowej i inne zabezpieczenia fizyczno-techniczne. Do podstawowych zabezpieczeń technicznych sprzętu komputerowego zalicza się listwy ochronne eliminujące zakłócenia napięcia występujące w sieci elektrycznej oraz zasilacze awaryjne UPS (zapewniające ciągłość zasilania energią elektryczną). Należy stosować również zabezpieczenia o charakterze administracyjno-organizacyjnym, w tym np. procedury fizycznej kontroli dostępu do pomieszczeń szczególnie ważnych, takich jak archiwum, serwerownia i dział informatyki. Niezbędne są także zabezpieczenia programowe w zakresie dostępu do komputerów i systemów informatycznych, a w szczególności dbałość o systematyczną zmianę haseł przez użytkowników systemów. Należy również przeprowadzać okresowe testowanie poprawności dysków twardych komputerów, aktualizować zabezpieczenia antywirusowe i antyspamowe.

W obecnych czasach należy się również spodziewać wielu różnych działań przestępczych z otoczenia zewnętrznego, które mogą być skierowane przeciwko dostępności informacji, integralności lub poufności. Są to takie działania, jak: *hacking*, *phishing*, *pharming*, rozpowszechnianie szkodliwego oprogramowania, niszczenie informacji, kradzież danych, wewnętrzny lub zewnętrzny sabotaż komputerowy, oszustwo komputerowe, fałszerstwo komputerowe, szpiegostwo komputerowe, podsłuch komputerowy, nielegalne uzyskiwanie i wykorzystywanie programu i wiele innych.

Z uwagi na to, że sytuacje awaryjne stanowią istotne zagrożenia dla zbiorów danych i innych zasobów informatycznych i mogą przynieść katastrofalne skutki dla jednostki, wiele podmiotów opracowuje politykę utrzymania ciągłości działania systemów lub plan ciągłości działania albo ustala co najmniej procedury postępowania w sytuacjach awaryjnych, takie jak (Szczepankiewicz, 2012):

- procedura postępowania pracowników w przypadkach awarii, wypadkach losowych i stanach zagrożenia;
- procedura przetwarzania danych w trybie awaryjnym w stanie zagrożenia lub po wypadku losowym – plan obejmujący procedury przetwarzania alternatywnego, stosowanego przejściowo do usunięcia przyczyn lub skutków;
- procedura działań po awarii w celu powrotu do stanu normalnego przetwarzania, m.in. procedury odtworzenia zbiorów danych lub programów z kopii rezerwowych.

Stosując się do wymagań UoR, kierownik jednostki musi również zadecydować o użyciu odpowiednich komputerowych nośników, które zapewnią trwałość zapisu danych i ksiąg rachunkowych. Przepisy ustawy wymagają także wdrożenia odpowiednich procedur programowych i organizacyjnych zapewniających ochronę danych i ksiąg rachunkowych. W praktyce jednostek wybór nośników do archiwizacji ksiąg rachunkowych oraz nośników do tworzenia bieżących rezerwowych kopii danych zawsze zależy od wielu czynników, m.in. od:

- skali działalności jednostki,
- liczby dziennych operacji rejestrowanych w systemie informatycznym rachunkowości,
- ważności gromadzonych danych,
- poziomu stosowanej w jednostce technologii informatycznej,
- posiadanych środków finansowych na system ochrony.

Małe jednostki stosują zwykle najtańsze sposoby archiwizowania danych. Kopie danych i ksiąg rachunkowych przechowują zazwyczaj na dyskach CD-R lub przenośnych dyskach twardych odpowiednio zabezpieczonych hasłem dostępu. Zwykle przechowują je w zabezpieczonym sejfie lub pomieszczeniu. Jednak w większości małych jednostek często brakuje pisemnych regulacji wewnętrznych w tym zakresie, które powinny być uwzględnione w polityce rachunkowości jednostki. Natomiast w wielu średnich i dużych jednostkach dość powszechnym sposobem przechowywania danych jest kopiowanie zbiorów danych finansowych na zapasowy serwer, który jest przeznaczony wyłącznie do tego celu i jest odpowiednio zabezpieczony w sposób programowy i fizyczny. Zasadniczo średnie i duże jednostki mają opracowane wytyczne w zakresie ochrony zasobów informatycznych rachunkowości, niekiedy są to dokumenty zwane polityką bezpieczeństwa systemów informatycznych lub polityką bezpieczeństwa informacji. Jednostki takie mają zazwyczaj ogólnie sformułowane wytyczne w tym zakresie w polityce rachunkowości jednostki.

Korporacje, instytucje finansowe i duże jednostki sektora finansów publicznych ze względu na skalę i znaczenie gromadzonych i przetwarzanych danych stosują znacznie droższe sposoby zabezpieczenia danych finansowych i ksiąg

rachunkowych w systemie informatycznym rachunkowości, np. archiwizowanie zbiorów danych we własnym specjalnie zabezpieczonym centrum (dziale, departamencie) przetwarzania danych albo zewnętrznym specjalistycznym centrum danych. Dla tego typu jednostek sposób ten stanowi bezpieczne rozwiązanie przechowywania danych informatycznych. Należy podkreślić, że zewnętrzne centra danych muszą stosować najnowsze technologie w zakresie przetwarzania, składowania, przesyłania i zabezpieczenia danych informatycznych swoich klientów.

Szczególnie ważnym ustawowym aspektem ochrony danych informatycznych jest systematyczne tworzenie bieżących rezerwowych kopii zbiorów danych w systemie informatycznym rachunkowości. Zabezpiecza ono przed możliwością utraty danych z przyczyn losowych, np. pożaru czy kradzieży sprzętu komputerowego. Prawidłowo organizowany proces wykonywania kopii rezerwowych wyróżnia się czterema cechami (Szczepankiewicz, 2012):

- regularnym cyklem tworzenia tych kopii,
- fizyczną odrębnością nośników, na których kopie te są tworzone,
- testowaniem możliwości odtworzenia danych z kopii (kontrola prawidłowości sporządzanych kopii),
- wyznaczonym, odpowiednio przystosowanym i zabezpieczonym miejscem do przechowywania sporządzonych tych kopii.

Należy pamiętać, że rezerwowe kopie danych umożliwią odtworzenie wszystkich zapisów jedynie według stanu na dzień utworzenia kopii. Zatem ważna jest częstotliwość tworzenia tych kopii. W praktyce jest ona różna i zależy od indywidualnej oceny problemów bezpieczeństwa w jednostce. Bierze się pod uwagę m.in.:

- ilość i ważność zgromadzonych danych,
- stopień zaufania do jakości sprzętu komputerowego i oprogramowania,
- czas potrzebny pracownikom do ponownego wprowadzenia utraconych danych do systemu informatycznego rachunkowości,
- występowanie dokumentów w postaci zapisu elektronicznego, które są wprowadzane za pośrednictwem urządzeń łączności lub komputerowych nośników danych i zależą od umiejętności użytkowników.

Niektóre systemy informatyczne rachunkowości stosowane w małych i średnich jednostkach mają wbudowaną funkcję informowania użytkownika o konieczności archiwizacji danych. W dużych jednostkach tworzenie kopii rezerwowych jest zazwyczaj uruchomiane automatycznie raz na dobę, po zakończeniu pracy przez wszystkich użytkowników, i jest nadzorowane z poziomu administratora systemu lub administratora serwera.

Zapis w polityce rachunkowości na temat bezwzględnego zapewnienia trwałości zapisu w jednostkach powinien dotyczyć jedynie tworzenia kopii zbiorów

ksiąg rachunkowych za rok obrotowy, jeśli mają być przechowywane w postaci zapisu elektronicznego. Ponadto, ze względu na możliwość uszkodzenia systemu informatycznego rachunkowości w czasie jego eksploatacji, jednostki tworzą kopie dysków CD zawierających oryginalną wersję oprogramowania do ponownego zainstalowania.

W wielu jednostkach przyjęto dobrą praktykę, że rezerwowe kopie danych i rezerwowe kopie oprogramowania przechowuje się w innych pomieszczeniach niż sprzęt, na którym są gromadzone dane oryginalne. W mniejszych jednostkach najczęściej wydziela się inne pomieszczenie lub specjalny sejf do przechowywania nośników danych (niekiedy ekranowany przed wpływem pól magnetycznych i odporny na ogień). W dużych jednostkach zazwyczaj są wydzielone w tym celu odrębne pomieszczenia lub działy.

Zgodnie z wytycznymi UoR rozwiązania programowe służące ochronie programów i danych systemu informatycznego rachunkowości opracowane przez jednostkę powinny uniemożliwić nieautoryzowany dostęp do programów, danych i sprzętu komputerowego, w wyniku którego mogłyby nastąpić: utrata danych lub programów, ujawnienie, pozyskanie lub nieupoważnione ich rozpowszechnienie. W praktyce najprostsza ochrona programowa systemu informatycznego rachunkowości polega na stosowaniu systemu haseł dostępu do (Szczepankiewicz, 2016):

- komputera (I poziom zabezpieczenia),
- systemu informatycznego rachunkowości (II poziom zabezpieczenia) i/lub
- wybranych funkcji systemu informatycznego rachunkowości (III poziom zabezpieczenia), np. przetwarzania danych osobowych, wynagrodzeń, sprawozdań.

Ponadto do podstawowych, występujących w praktyce rozwiązań programowych należy zaliczyć wyposażenie systemu informatycznego rachunkowości w specjalne procedury (Szczepankiewicz, 2016):

- kontroli kompletności zbiorów danych,
- weryfikacji obliczeń,
- badania zgodności sum kontrolnych,
- powiązań rachunkowych i logicznych między zbiorami.

Stosowanie wyżej wymienionych procedur umożliwia automatyczne wykrywanie niespójności danych w treści zbiorów danych, weryfikację przetwarzania i ujawnienie prób ingerencji w ich zawartość po modyfikacji innym narzędziem niż system informatyczny rachunkowości.

Należy podkreślić, że UoR nie wymienia również, jakie rozwiązania o charakterze organizacyjno-administracyjnym należy przyjąć do ochrony zasobów informatycznych rachunkowości. W praktyce zakres tych rozwiązań jest również

kształtowany w zależności od specyfiki działalności jednostki, stosowanych rozwiązań informatycznych, a niekiedy także przeprowadzonej analizy ryzyka informatycznego.

W wielu jednostkach zabezpieczenia na poziomie organizacyjno-administracyjnym dotyczą takich obszarów, jak:

- ustalenie trybu wdrażania nowych wersji programów;
- wyraźne rozdzielenie obowiązków i kompetencji między użytkowników systemu informatycznego rachunkowości;
- szkolenie pracowników, przestrzeganie tajemnicy służbowej, kontroli działań użytkowników systemów, właściwe postępowaniu przy zwalnianiu pracownika;
- zabezpieczenie archiwizowanej dokumentacji i zbiorów danych.

Przed przyjęciem systemu informatycznego rachunkowości do eksploatacji należy go przetestować w celu oceny jego zgodności z wymogami UoR oraz kompletności i poprawności realizowania funkcji, do których został przewidziany. Podczas testowania można stwierdzić m.in., czy system poprawnie realizuje wszystkie zaprojektowane funkcje, bezwarunkowo odrzuca błędne dane w procesie wprowadzania ich przez użytkownika, posiada wbudowane testy poprawności działań i sumy kontrolne oraz bada kompletność zbiorów. Jako dokument potwierdzający przetestowanie i dopuszczenie systemu informatycznego rachunkowości do użytkowania należy sporządzić stosowny protokół lub inny dokument dołączony do dokumentacji ewidencyjnej oprogramowania eksploatowanego w jednostce wymienionej w art. 10 UoR.

Kolejnym ważnym praktycznym aspektem ochrony zasobów informatycznych rachunkowości jest rozdzielenie obowiązków i kompetencji pomiędzy użytkowników systemu informatycznego rachunkowości. Z organizacyjnego punktu widzenia w większych jednostkach różnicuje się prawa dostępu do systemu informatycznego rachunkowości poprzez nadanie uprawnień każdemu użytkownikowi stosownie do przydzielonego zakresu czynności, by mógł wykonywać powierzone obowiązki. Niekiedy w systemie informatycznym rachunkowości ogranicza się również dostęp wyłącznie do wyznaczonych funkcji systemu lub obsługi określonych grup danych (np. wcześniej wspomnianych danych osobowych, wynagrodzeń, sprawozdań).

W praktyce w wielu jednostkach wyznacza się również osobę uprawnioną (np. głównego księgowego lub administratora systemu) do przydzielania uprawnień, wprowadzania zmian lub zawieszania uprawnień użytkownikom w systemie informatycznym rachunkowości. Osoba zarządzająca uprawnieniami powinna prowadzić rejestr użytkowników systemu informatycznego rachunkowości. Rejestry takie powinny ujmować kilkuletnią historię dostępu wszystkich użytkowników do kolejnych, zmodyfikowanych wersji SIR eksploatowanych w jednostce.

UoR wymaga również, by system informatyczny rachunkowości identyfikował użytkownika, który wprowadził lub modyfikował dane w systemie. Każdy użytkownik systemu ma przypisaną tzw. sygnaturę umożliwiającą identyfikację osoby, która zaewidencjonowała lub zmodyfikowała dokument w systemie, zaksięgowała wprowadzony dokument lub zaksięgowała zapis stornujący dokumentu księgowego (zgodnie z art. 21, ust. 1, pkt 6 UoR). Sygnatura pojawia się na wszystkich wydrukach.

W wielu jednostkach użytkownikowi, który pracował w systemie informatycznym rachunkowości, a został przeniesiony na inne stanowisko lub rozwiązał umowę o pracę, trwale blokuje się dostęp do systemu przez zlikwidowanie jego uprawnień lub zmianę hasła. Danych identyfikacyjnych takiego użytkownika nie usuwa się z systemu. Sygnatura i nazwisko zablokowanego użytkownika pozostają w systemie informatycznym rachunkowości, aby umożliwić identyfikację wcześniej wprowadzonych, modyfikowanych i księgowanych przez niego dokumentów.

W praktyce przyjęto również, że procedury ochrony zasobów informatycznych rachunkowości zobowiązują użytkowników systemu informatycznego rachunkowości do pisemnego potwierdzenia m.in.:

- zapoznania się z zasadami zawartymi w instrukcjach obsługi sprzętu i podręcznikach użytkownika systemu informatycznego rachunkowości;
- ochrony danych i sprzętu komputerowego przed nieautoryzowanym dostępem, w szczególności do okresowej zmiany haseł dostępu;
- przestrzegania zakazu instalacji oprogramowania nielicencjonowanego i oprogramowania nieprzeznaczonego do celów służbowych oraz dokonywania jakichkolwiek zmian w zainstalowanych programach;
- kontroli antywirusowej wszelkich stosowanych nośników danych;
- uszkadzania dysków, innych informatycznych nośników i wydruków przeznaczonych do likwidacji w sposób uniemożliwiający odczytanie zawartych na nich danych.

W niektórych jednostkach sporządza się także inne dodatkowe procedury związane z ochroną i eksploatacją systemu informatycznego rachunkowości, np. instrukcję dotyczącą fizycznego transportu nośników danych i ich przechowywania. Instrukcja dotycząca fizycznego transportu nośników danych dotyczy zarówno dokumentów papierowych, jak i danych umieszczonych na nośnikach komputerowych. Powinna określać środki zabezpieczenia związane zarówno z transportem wewnętrznym, jak i zewnętrznym (np. do zewnętrznego ośrodka obliczeniowego, biura rachunkowego). Zazwyczaj reguluje ona zagadnienia dotyczące właściwości opakowań nośników; wykazu i zasad sporządzania dokumentów towarzyszących transportowi; sprawdzania tożsamości odbiorcy nośników i potwierdzenia odbioru na dokumentach spedycji; zasad

obsługi transportu; harmonogramu transportu oraz niezawodności środków transportu. Jednostki sporządzają również odpowiednie instrukcje spedycji oraz dokumenty towarzyszące spedycji. Dokumenty te zawierają zazwyczaj następujące informacje:

- nazwę jednostki (komórki organizacyjnej) przygotowującej nośniki;
- nazwę lub symbol systemu informatycznego rachunkowości, z którego dane pochodzą; rodzaje nośników;
- liczbę egzemplarzy nośników i sumy kontrolne;
- datę przekazania nośników;
- określenie osoby przekazującej i odbierającej nośniki.

Ponadto należy zwrócić uwagę na to, że jesli chodzi o zabezpieczenie archiwizowanej dokumentacji i zbiorów danych, w tym ksiąg rachunkowych, to z prawnego punktu widzenia nie ma różnicy, czy w wyniku nieprawidłowego przechowywania jednostka utraciłaby księgi rachunkowe sporządzone w postaci wydruków czy zachowane na komputerowych nośnikach danych. Dlatego w praktyce wielu jednostek dużo bezpieczniejsze, szybsze i tańsze okazało się przenoszenie danych na komputerowe nośniki danych oraz umieszczenie ich w sejfie jednostki albo skrytce bankowej niż drukowanie czasem setek stron i przechowywanie w wielu szafach, przez co najmniej sześć lat. Jednak warunkiem koniecznym przechowywania tych zasobów w postaci elektronicznej powinien być obowiązek przeprowadzenia testu możliwości odtworzenia danych z kopii, czyli kontrola, czy kopie zostały prawidłowo sporządzone.

5.3. Polityka rachunkowości w zakresie ochrony zasobów informatycznych

Politykę (zasady) rachunkowości w szerokim znaczeniu można zdefiniować jako zbiór standardów rachunkowości, interpretacji, metod, reguł i praktyk oraz przepisów wykorzystywanych przez jednostkę do prowadzenia rachunkowości i sporządzania sprawozdań finansowych. W węższym znaczeniu polityka rachunkowości odnosi się do sytuacji, w których określone standardy pozostawiają jednostce prawo swobodnego wyboru rozwiązań. Wówczas w polityce rachunkowości znajdą się przyjęte przez jednostkę wybrane zasady, sposoby i procedury postępowania w systemie rachunkowości wybrane spośród wielu dopuszczalnych rozwiązań, które są dostosowane do potrzeb jednostki (Kabalski, 2009). Takim obszarem regulacji zawartym w polityce rachunkowości jest system ochrony danych księgowych, systemów ich przetwarzania i sprzętu komputerowego wykorzystywanego do prowadzenia rachunkowości.

W zakresie ochrony zasobów informatycznych rachunkowości w jednostkach ustanowienie polityki (zasad) rachunkowości oraz ich stosowanie ma na celu m.in.:

- zabezpieczenie jednostki przed utratą danych finansowych lub ich uszkodzeniem w stopniu uniemożliwiającym dalszą kontynuację działalności;
- uniemożliwienie nieautoryzowanego dostępu do systemu informatycznego rachunkowości i jego danych, w wyniku którego mogłoby nastąpić ich pozyskanie, ujawnienie lub nieupoważnione rozpowszechnienie;
- zminimalizowanie strat związanych z utratą sprzętu komputerowego wraz z danymi w wyniku zdarzeń losowych (kradzież, pożar, powódź itp.).

Niezwykła złożoność problematyki i indywidualny charakter rozwiązań w zakresie bezpieczeństwa zasobów informatycznych rachunkowości przyjmowanych w poszczególnych jednostkach powoduje, że kierownicy jednostek, opracowując politykę rachunkowości w tym obszarze, poza stosowaniem się do przepisów UoR uwzględniają także wiele innych aspektów praktycznych. Planowanie właściwego systemu ochrony zasobów informatycznych rachunkowości w jednostce musi uwzględniać specyfikę zarówno prowadzonej działalności, jak i stosowanych rozwiązań informatycznych dla potrzeb prowadzenia rachunkowości. Z tego względu w wielu jednostkach przed przyjęciem odpowiedniego systemu zabezpieczeń na poziomie fizyczno-technicznym i organizacyjno-administracyjnym oraz programowym najpierw przeprowadza się analizę prawdopodobieństwa wystąpienia określonych rodzajów ryzyka informatycznego, szacuje się wartość potencjalnej utraty danych, oprogramowania czy sprzętu informatycznego, jak również bada się znaczenie takich zdarzeń dla kontynuacji działalności jednostki oraz szacuje ewentualny koszt otworzenia danych po ich utracie. Wnioski z tych analiz powinny znaleźć odzwierciedlenie w przyjęciu odpowiednich zasad ochrony zasobów informatycznych w polityce rachunkowości. Należy jednak pamiętać, że zasady ochrony zasobów informatycznych rachunkowości powinny podążać za rozwojem informatyki w jednostce, a zatem muszą być również aktualizowane w polityce rachunkowości.

Ze względu na wielość rozwiązań praktycznych w jednostkach trudno jest zaprezentować jednolity wzór dokumentu polityki rachunkowości w omawianym zakresie. Jednakże bezwzględnie w każdej polityce rachunkowości zgodnie z wymaganiami UoR powinny się znaleźć zasady określające system ochrony zasobów informatycznych rachunkowości, w tym co najmniej o systematycznym tworzeniu rezerwowych kopii danych księgowych oraz technicznej, programowej i organizacyjnej ochronie tych zasobów.

Przykładową treść polityki rachunkowości w części opisującej system ochrony dokumentów i ksiąg rachunkowych w systemie informatycznym rachunkowości prezentuje poniższy wzór dokumentu.

Polityka rachunkowości w zakresie systemu ochrony dokumentów i ksiąg rachunkowych w systemie informatycznym rachunkowości

A. System ochrony dokumentów i ksiąg rachunkowych w systemie informatycznym rachunkowości

I. Fizycznemu i organizacyjnemu zabezpieczeniu, które zapewnia ochronę przed dostępem osób nieupoważnionych, niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem w systemie rachunkowości podlegają:
   1) sprzęt komputerowy wspomagający rachunkowość jednostki,
   2) zintegrowany informatyczny system rachunkowości, składający się z podsystemów: finansowo-księgowego, kadrowego-płacowego, ewidencji środków trwałych,
   3) rezerwowe kopie danych (zapisów dokumentów księgowych w systemie informatycznym rachunkowości),
   4) polityka (zasady) rachunkowości,
   5) księgi rachunkowe,
   6) dowody księgowe,
   7) dokumentacja inwentaryzacyjna,
   8) sprawozdania finansowe.

II. Wszystkie pomieszczenia, w których użytkowany jest sprzęt komputerowy z systemem informatycznym rachunkowości, zamykane są na klucz. Po zakończeniu pracy użytkownicy systemu informatycznego rachunkowości klucze oddają do portierni. Po godzinach pracy w pomieszczeniach przebywać może tylko osoba sprzątająca lub pracownik posiadający zezwolenie kierownika jednostki na pracę w innych godzinach niż wyznaczone godziny pracy albo w dniach wolnych od pracy. Dostęp do systemu informatycznego rachunkowości i innych systemów informatycznych mają osoby posiadające uprawnienia nadane przez administratora systemu. Administratorem systemów w jednostce jest: ……

III. Szczegółowe instrukcje zarządzania eksploatacją systemu informatycznego rachunkowości oraz stosowne procedury dla systemu finansowo-księgowego, systemu kadrowego-płacowego, ewidencji środków trwałych, ……, określają:
   1) rejestr uprawnień użytkowników korzystania z poszczególnych podsystemów systemu informatycznego rachunkowości,
   2) procedury tworzenia rezerwowych kopii zbiorów danych oraz instrukcje programów i narzędzi programowych służących do ich przetwarzania,
   3) harmonogram sporządzania rezerwowych kopii danych ustalany jest przez kierownika działu informatyki i obowiązuje przez cały czas trwania eksploatacji podsystemów systemu informatycznego rachunkowości.

IV. Codziennie wykonywane są kopie bazy danych do pliku na serwerze. Kopia cykliczna dzienna przechowywana jest przez okres 1 tygodnia, kopia miesięczna przez 3 miesiące, roczna przez 5 lat. Raz na kwartał testuje się możliwość odtworzenia danych z kopii (kontrola prawidłowości sporządzanych kopii).

V. Dostęp do nośników z kopiami mają tylko pracownicy działu informatyki. Kopie przechowywane są sejfie w budynku X (innym niż siedziba główna), do którego dostęp mają tylko osoby posiadające stosowne upoważnienia. Bazy dodatkowo archiwizowane są na taśmach magnetycznych w cyklu tygodniowym, miesięcznym i rocznym. Dodatkowo dane księgowe archiwowane są na płytach CD-R, które umożliwiają każdorazowo ich odczyt oraz wydruk. Archiwizowania na płyty CD-R dokonuje wyznaczony pracownik księgowości we współpracy z administratorem systemu po zakończeniu kwartału każdy miesiąc oddzielnie. Sporządzane są dwie kopie, z których jedna przechowywana jest w podręcznej kasie pancernej w archiwum

księgowości, druga natomiast w sejfie umieszczonym w budynku …….. Dostęp do sejfu w tym budynku mają osoby posiadające stosowne upoważnienia.

VI. Zintegrowana baza danych systemu informatycznego rachunkowości jest zainstalowana na serwerze pod kontrolą systemu operacyjnego ……(np. MS Windows, Linux, UNIX itp.) i wymaga systematycznej ochrony wirusowej i antyspamowej. Przed nieuprawnionym dostępem baza danych chroniona jest poprzez odpowiednią konfigurację sprzętową oraz przez reguły FireWalla.

VII. Podsystemy systemu informatycznego rachunkowości są zabezpieczone przed utratą danych spowodowanych awarią zasilania poprzez podłączenie do zasilaczy awaryjnych UPS. W przypadku awarii zasilania serwer może pracować nie mniej niż 15 minut, co pozwala na jego bezpieczne wyłączenie.

VIII. Ochrona danych w trakcie pracy systemu informatycznego rachunkowości zapewniona jest poprzez:

1) zorganizowanie komunikacji za pomocą relacji klient–serwer, wykluczającej bezpośredni dostęp użytkowników do zasobów serwera,
2) stosowanie systemu identyfikatorów i haseł znanych wyłącznie użytkownikom podsystemów systemu informatycznego rachunkowości,
3) zdefiniowanie indywidualnych uprawnień użytkowników w zakresie użytkowania poszczególnych podsystemów SIR oraz funkcji i zasobów programu,
4) wyznaczenie administratora systemu (informatyka) odpowiedzialnego za codzienne, systemowe archiwowanie danych, tworzenie rezerwowych kopii danych, funkcjonowanie serwera i zasilania sprzętu komputerowego i innych urządzeń wspomagających eksploatację systemu informatycznego rachunkowości,
5) sporządzanie kopii przed każdą zmianą wersji podsystemów, a także przed złożoną operacją związaną z ryzykiem utraty lub zakłócenia zawartości zbiorów danych,
6) przekazywanie do przechowywanie w budynku ….. kopii zbiorów ksiąg rachunkowych sporządzonej po zamknięciu każdego roku,
7) przechowywanie oprogramowania instalacyjnego, licencji i dokumentacji systemu w zabezpieczonym pomieszczeniu działu informatyki,
8) zapewnienie stosowania możliwie najnowocześniejszych rozwiązań technicznych i programowych w zakresie zabezpieczenia pracy serwera, podtrzymywania zasilania i sprawności sieci informatycznej.

IX. W jednostce obowiązuje Instrukcja obiegu i kontroli dokumentów. Dokumenty księgowe przekazywane są do archiwum zakładowego. Przekazanie akt odbywa się na podstawie protokołu zdawczo-odbiorczego. Akta są opisane zgodnie z zarządzeniem wewnętrznym kierownika jednostki oraz w sprawie Instrukcji kancelaryjnej, Instrukcji o organizacji i zakresie działania Archiwum oraz Jednolitego rzeczowego wykazu akt. Bieżące dokumenty księgowe w jednostce przechowywane są w archiwum podręcznym księgowości. Dostęp do archiwum oraz możliwości korzystania z jego zasobów określa Instrukcja korzystania z archiwum podręcznego księgowości.

B. Okresy przechowywania zbiorów danych z systemu informatycznego rachunkowości

I. Okresowemu przechowywaniu podlegają:
   1) dokumentacja przyjętego sposobu prowadzenia rachunkowości – przez okres nie krótszy niż 5 lat od upływu ich ważności,
   2) karty wynagrodzeń pracowników bądź ich odpowiedniki – przez okres wymaganego dostępu do tych informacji wynikający z przepisów emerytalnych, rentowych i podatkowych, nie krócej jednak niż 5 lat (maksymalnie 50 lat),

3) księgi rachunkowe, dokumenty inwentaryzacyjne oraz pozostałe dowody księgowe i dokumenty systemu informatycznego rachunkowości – przez okres 5 lat.

Powyższe terminy oblicza się od początku roku następującego po roku obrotowym, którego dane zbiory (dokumenty) dotyczą. Okres przechowywania pozostałej dokumentacji niearchiwalnej liczy się w pełnych latach kalendarzowych, poczynając od 1 stycznia roku następnego po utracie przez te dokumentacje praktycznego znaczenia dla potrzeb jednostki oraz celów kontrolnych.

II. Księgi rachunkowe mają formę zapisów na komputerowych nośnikach danych. Zbiory przechowywane są w sposób należyty i chronione przed niedozwolonymi zmianami, rozpowszechnianiem, uszkodzeniem lub zniszczeniem. Przed umieszczeniem w archiwum testuje się możliwość odtworzenia danych z kopii (kontrola prawidłowości sporządzanych kopii) pod nadzorem informatyka i głównego księgowego.

C. Udostępnianie danych i dokumentów z systemu informatycznego rachunkowości

Udostępnienie sprawozdań finansowych, dowodów księgowych, ksiąg rachunkowych oraz innych dokumentów z systemu informatycznego rachunkowości może nastąpić:

1) na potrzeby wewnętrzne – w siedzibie jednostki do wglądu po uzyskaniu zgody głównego księgowego,
2) na zewnątrz – po uzyskaniu pisemnej zgody kierownika jednostki i pozostawieniu pisemnego pokwitowania zawierającego spis wydanych dokumentów.

Źródło: (Szczepankiewicz, 2012, s. 106–108).

Podsumowanie

Problemy zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości powinny być jedną z głównych dziedzin zainteresowania kierownika jednostki. Musi on pamiętać o konieczności skutecznej ochrony przed nieuprawnioną i niekontrolowaną modyfikacją, wprowadzeniem lub usunięciem zapisów księgowych. UoR wychodzi naprzeciw potrzebom jednostek, umożliwiając obecnie bardzo dużą dowolność w kształtowaniu procedur oraz mechanizmów zabezpieczeń zasobów informatycznych rachunkowości z wykorzystaniem najnowszych zdobyczy informatyki.

Ponadto należy mieć na uwadze, że w ostatnich latach większe znaczenie podczas audytu zyskała ocena systemu kontroli wewnętrznej i systemu informatycznego rachunkowości. Audyt obejmuje ocenę ryzyka informatycznego, a także ocenę poprawności oprogramowania, jego funkcjonalnych mechanizmów kontrolnych i algorytmów przetwarzania danych oraz związaną z tym dokumentację. Ponadto audytowana jest dokumentacja ewidencyjna systemu informatycznego rachunkowości, opis systemu ochrony zasobów informatycznych rachunkowości oraz zastosowane zabezpieczenia fizyczno-techniczne, organizacyjno-administracyjne i programowe. Ocenie podlega praktyczne przestrzeganie najważniejszych zasad, m.in.: systematycznego tworzenia re-

zerwowych kopii danych, konfiguracji haseł i sposób przydzielania uprawnień dostępu do zasobów oraz sprawowania nadzoru nad służbami informatycznymi i użytkownikami systemu informatycznego rachunkowości. Audytor ocenia również techniczne bezpieczeństwo sprzętu komputerowego oraz posiadanie procedur postępowania w sytuacjach awaryjnych.

Bibliografia

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

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

Dudek, M. i Szczepankiewicz, E. I. (2009). Rozwój technologii informatycznych a zagrożenia i zarządzanie bezpieczeństwem informacji w przedsiębiorstwach. W: M. Grzybowski i J. Tomaszewski (red.), *Logistyka, komunikacja, bezpieczeństwo: wybrane problemy* (s. 263–274). Wydawnictwo Wyższej Szkoły Administracji i Biznesu (WSAiB) im. E. Kwiatkowskiego w Gdyni.

Kabalski, P. (2009). *Polityka rachunkowości w spółce stosującej MSSF*. Stowarzyszenie Księgowych w Polsce.

Szczepankiewicz, E. I. (2012). Praktyka jednostek a polityka rachunkowości w zakresie ochrony zasobów informatycznych rachunkowości. W: M. Wrona i W. Janik (red.), *Polityka rachunkowości w teorii i w praktyce* (s. 91–110). Wydawnictwo KUL.

Szczepankiewicz, E. I. (2014). Audyt sprawozdań finansowych w środowisku informatycznym. W: W. Gabrusewicz (red.), *Audyt sprawozdań finansowych. Teoria i praktyka* (s. 228–266). Polskie Wydawnictwo Ekonomiczne.

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

Szczepankiewicz, E. I. (2019). *Kontrola zarządcza w jednostkach samorządu terytorialnego. Ocena i doskonalenie procedur kontroli zarządczej w środowisku informatycznym rachunkowości*. CONTACT.

Ustawa. (2023). Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2023r., poz. 120, 295, 1598).

Ustawa. (2000). Ustawa z dnia 9 listopada 2000 r. o zmianie ustawy o rachunkowości (Dz. U. Nr 113, poz. 1186).