Piotr Pisarewicz*

Analiza wymogów i regulacji w zakresie tworzenia, przechowywania i zabezpieczania dokumentów bankowych w kontekście ochrony interesu klientów

Wstęp

Ochrona interesu klientów jest w sektorze finansowym jedną z istotniejszych kwestii i wyzwań ostatnich dekad. Globalizacja rynków oraz postęp technologiczny skutkują internacjonalizacją i znacznym wzrostem liczby transakcji, jak i przyspieszeniem tempa ich realizacji. Powoduje to z kolei wzrost prawdopodobieństwa wszelkiego rodzaju nadużyć powodowanych zarówno przez same instytucje finansowe, jak i przez czynniki zewnętrzne. Jednym z kluczowych wątków w tym zakresie jest szeroko pojęta ochrona dokumentacji, która winna zabezpieczać klientów instytucji finansowych przed utratą środków pieniężnych oraz innymi konsekwencjami naruszeń treści zawartych umów. Należy zwrócić uwagę, iż większość dokumentacji będących podstawą zawieranych transakcji ma już formę elektroniczną [Krzyżkiewicz, 2008, s. 330–332]. To z kolei powoduje szereg nowych ryzyk właściwych dla tego typu nośników informacji. Przykładem w tym zakresie może być sektor bankowy, który w ostatnich latach narażony jest w szczególny sposób na próby łamania systemów informatycznych, nieuprawnione i nieautoryzowane próby dostępu do rachunków klientów itp. Wspomniane wcześniej czynniki globalizacyjne i technologiczne w znacznym stopniu ułatwiają różnego rodzaju osobom oraz organizacjom przestępczym nielegalne pozyskiwanie środków. Liczne ataki na systemy informatyczne stanowią ogromne wyzwanie dla każdego banku zarówno w Polsce, jak i w innych krajach.

Biorąc pod uwagę powyższe kwestie, autor podjął decyzję o przeprowadzeniu analizy adekwatności wymogów i regulacji w zakresie tworzenia, przechowywania i zabezpieczania dokumentów bankowych w kontekście ochrony interesu klientów. Uwaga skupiona została na rynku krajowym, a zakres analizy objął zarówno obecne, jak i historyczne brzmienia dokumentów formalnoprawnych wiążących rodzime banki

* Dr, Katedra Finansów i Ryzyka Finansowego, Wydział Zarządzania, Uniwersytet Gdański, ul. Armii Krajowej 101, 81-824 Sopot, piotr.pisarewicz@wp.pl

w wyżej wskazanym zakresie. To pozwoliło na ocenę ewolucji i zmian, które były efektem szybkiego rozwoju sektora bankowego. Ograniczone ramy artykułu nie pozwoliły na kompleksowe opisanie badanych zagadnień, niemniej jednak w opracowaniu dokonano syntezy najważniejszych kwestii, które determinują w praktyce bankowej wyżej wskazane zagadnienie. Przegląd i analiza aktów prawnych objęła dokumenty na poziomie ustaw, rozporządzeń, jak i aktów tzw. miękkiego prawa, które na mocy obowiązujących przepisów mogą być wydawane przez organ nadzoru. Powyższe zagadnienia ujęto w trzech kolejnych rozdziałach opisujących najważniejsze elementy i szczegóły przeprowadzonych badań.

1. Ochrona dokumentacji a Prawo bankowe

Pierwszy akt prawny, który poddano analizie pod kątem badanych zagadnień, to ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe. Jest to kluczowy dokument wyznaczający zasady funkcjonowania i standardy systemu bankowego w Polsce, a jednocześnie podstawowy akt prawny wyznaczający standardy w zakresie tworzenia, przechowywania i zabezpieczania dokumentacji bankowej. Globalne trendy i postęp technologiczny spowodowały, iż ustawa zawiera postanowienia, na mocy których wszelkie oświadczenia woli dotyczące czynności bankowych mogą być realizowane w postaci elektronicznej. Niemniej jednak mogą być one sporządzane na informatycznych nośnikach danych, tylko jeżeli dokumenty będą w sposób należyty utworzone, utrwalone, przekazane, przechowywane i zabezpieczone. Kluczowym wyzwaniem w tym zakresie jest właściwe przechowywanie i zabezpieczenie dokumentacji, które może być realizowane w praktyce przez same banki, ale także przez spółki w ramach grup kapitałowych oraz przez tzw. przedsiębiorstwa pomocniczych usług bankowych. Znamienne jest to, iż gdy ustawa zastrzega dla czynności prawnej formę pisemną, to uznaje się, że czynność dokonana w formie elektronicznej spełnia wymagania formy pisemnej, nawet gdy forma taka została zastrzeżona pod rygorem nieważności. Ustawodawca postanowił nadto, iż sposób tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania dokumentów (w tym przy zastosowaniu podpisu elektronicznego) w celu zapewnienia ich bezpieczeństwa określić ma Rada Ministrów w drodze odrębnego rozporządzenia [ustawa, 1997, art. 7 ust. 1–4]. Efektem zapisu ustawowego było uchwalenie rozporządzenia Rady Ministrów z dnia 25 lutego 2003 r. w sprawie zasad tworzenia, utrwalania, przechowywania i zabezpieczania, w tym przy za-

stosowaniu podpisu elektronicznego, dokumentów bankowych sporządzanych na elektronicznych nośnikach informacji. Głównym zadaniem dokumentu było zapewnienie maksymalnego stopnia bezpieczeństwa dokumentów bankowych oraz ochrona interesów banków oraz samych klientów.

Klasyczna, czyli papierowa, forma dokumentów rzecz jasna także może funkcjonować z powodzeniem we współczesnej praktyce bankowej. Potwierdzają to postanowienia ustawy umożliwiające bankom wydawanie ich w tej właśnie formie posiadaczom rachunków oszczędnościowych, terminowych lokat oszczędnościowych, imiennych książeczek oszczędnościowych lub innych dokumentów potwierdzających zawarcie umów. Należy zaznaczyć, iż w takim przypadku banki nie są już zobligowane do wysyłania ich posiadaczom wyciągów bankowych. W razie ich utraty lub zagubienia dokumenty tego typu podlegają umorzeniu zgodnie z postanowieniami odrębnego rozporządzania Ministra Sprawiedliwości [ustawa, 1997, art. 53 ust. 1–4]. Na mocy zapisów ustawy uchwalone zostało rozporządzenie Ministra Sprawiedliwości z dnia 27 września 2004 r. w sprawie warunków i trybu umarzania dokumentów potwierdzających zawarcie umowy rachunku oszczędnościowego oraz rachunku terminowej lokaty oszczędnościowej.

Stosowne przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego i przepisy o postępowaniu egzekucyjnym w administracji określają tryb umarzania utraconych dokumentów zawarcia umów rachunków oszczędnościowych, oszczędnościowo-rozliczeniowego lub terminowych lokat oszczędnościowych w trybie egzekucji sądowej lub administracyjnej [ustawa, 1997, art. 62]. Widać więc, iż ustawodawca wskazał w Prawie bankowym liczne delegacje do innych aktów prawnych, regulujące szczegółowe aspekty poszczególnych obszarów aktywności banków.

Kolejną kluczową kwestią dla bezpieczeństwa klientów jest prawidłowa identyfikacja ich tożsamości przed złożeniem oświadczenia woli i dokonaniem transakcji. Ten element reguluje wymóg ustawy nakładający na banki obowiązek rzetelnego sprawdzania autentyczności i prawidłowości formalnej dokumentów będących podstawą wypłaty środków, jak i weryfikacji tożsamości osób przekazujących dane zlecenie [ustawa, 1997, art. 65]. Przedmiotem wielu sporów sądowych z bankami były i są nadal nieautoryzowane wypłaty i inne transakcje przeprowadzane z osobami do tego nieuprawnionymi. Ze względu na ich charakter

dokładne dane na temat liczby i wartości sporów nie były i nie będą najprawdopodobniej nigdy (a przynajmniej w najbliższej przyszłości) dostępne. Ich ujawnienie stanowiłoby dla banków daleko idący problem związany z utratą lub obniżeniem reputacji i zaufania klientów co do ich wiarygodności, co w kontekście globalizacji rynków skutkować mogłoby zmianą dostawcy usług [Smyczek, 2012, s. 129–133]. Sprawy tego typu są w praktyce na ogół rozwiązywane polubownie lub w drodze postępowania cywilnego bądź w ekstremalnych przypadkach nawet karnego. O ile dana sprawa jest rozpatrywana na szczeblu postępowania sądowego, może trwać nawet przez kilka lat, ponieważ obie strony sporu na ogół posiłkują się różnymi argumentami prawnymi i opiniami biegłych, co znacząco wydłuża całą procedurę.

Formalną podstawą do uznania mocy prawnej dokumentów w zakresie czynności bankowych, ustanowionych zabezpieczeń oraz wpisów w księgach wieczystych są:

– księgi rachunkowe banków,
– sporządzone na ich podstawie wyciągi,
– inne oświadczenia podpisane przez osoby upoważnione do składania oświadczeń w zakresie praw i obowiązków majątkowych banków i opatrzone pieczęcią banku,
– sporządzone w ten sposób pokwitowania odbioru.

Swoistym wyjątkiem od reguły jest ustawowe wyłączenie ww. dokumentów z mocy prawnej w postępowaniu cywilnym. Delegacja ustawowa w zakresie wymogów dotyczących identyfikacji banków w systemie teleinformatycznym, podpisu elektronicznego, korespondencji elektronicznej oraz bezpieczeństwa odsyła do stosownego rozporządzenia Ministra Finansów [ustawa, 1997, art. 65 ust. 1–2]. Powyższe zagadnienia wyczerpują najważniejsze zapisy Prawa bankowego w zakresie problemu badawczego. W następnych częściach analizie poddane zostaną kolejne akty prawne.

2. Tworzenie, zabezpieczanie i przechowywanie dokumentacji a przepisy o rachunkowości

W zakresie przepisów o rachunkowości analizie poddano dwa podstawowe akty prawne dotyczące wymogów w zakresie tworzenia, zabezpieczania i ustawowego okresu przechowywania dokumentów. Zbadano zatem stosowne zapisy rozporządzenia Ministra Finansów w sprawie szczególnych zasad rachunkowości banków oraz ustawy o rachunkowości.

2.1. Wymogi rozporządzenia Ministra Finansów

Jako punkt wyjścia w zakresie specyfiki rachunkowości banków zweryfikowano zapis § 32 ust. 1–2 rozporządzenia Ministra Finansów z dnia 10 grudnia 2001 r. w sprawie szczególnych zasad rachunkowości banków:

„1. Bank przestrzega zasad dotyczących przechowywania i ochrony danych określonych w przepisach art. 71 ustawy i odrębnych przepisach, z zastrzeżeniem ust. 2.
2. Bank przechowuje dowody księgowe w oryginalnej postaci przez okres wynikający z przepisu art. 74 ustawy (…)".

Przywołany powyżej § 32 rozporządzenia odnosi się do art. 71 oraz 74 ustawy o rachunkowości, które regulują szczegółowo kwestie związane z przechowywaniem, zabezpieczaniem, a także okresem przechowywania dokumentacji. Należy podkreślić, iż w tym zakresie banki traktowane są zgodnie z nadrzędnym przepisem ustawowym na równych zasadach, tak jak inne podmioty gospodarcze.

Znamienny jest także kolejny zapis rozporządzenia dotyczący możliwości udostępniania przez banki dokumentów osobom trzecim. W tym zakresie wymagane jest zachowanie przepisów dotyczących tajemnicy bankowej lub uzyskanie zgody kierownika jednostki organizacyjnej banku na wgląd w dokumenty na miejscu. Dodatkowym wymaganym kryterium jest wydanie pisemnej zgody prezesa zarządu banku lub osoby przez niego upoważnionej na udostępnienie dokumentów poza miejscem prowadzenia ksiąg rachunkowych. Warunkiem w tym zakresie jest pozostawienie potwierdzonych „za zgodność z oryginałem" fotokopii dokumentów i protokołu zawierającego ich wykaz [rozporządzenie, 2001, § 32 ust. 3]. Autor, przeprowadzając analizę historyczną aktów prawnych, stwierdził, iż analogicznie ww. kwestie ujmowały kolejne nowelizacje rozporządzenia Ministra Finansów w sprawie szczególnych zasad rachunkowości banków: z dnia 29 sierpnia 2008 r. oraz 1 października 2010 r., świadcząc o stabilności prawa w tym zakresie, choć zapisy znajdują się w nieco innym fragmencie tekstu [rozporządzenie, 2010, § 49 ust. 1–3]. Należy także zwrócić uwagę, iż w bankach lub wyodrębnionych spółkach grup kapitałowych bywa prowadzona działalność maklerska, która także wymaga stosownego zabezpieczania dokumentacji [Krzyżkiewicz, 2008, s. 323–326]. W takich przypadkach zastosowanie ma rozporządzenie Ministra Finansów z dnia 18 grudnia 2001 r. w sprawie szczególnych zasad rachunkowości domów maklerskich i jednostek organizacyjnych banków,

w ramach których prowadzona jest działalność maklerska. W dokumencie tym także widnieją stosowne fragmenty i wymogi dotyczące zabezpieczania dokumentów, niemniej ze względu na specyfikę nie będą szerzej omawiane.

2.2. Wymogi ustawy o rachunkowości

Poniżej zostaną omówione przepisy art. 71 ustawy o rachunkowości do których odnosi się wspomniany uprzednio § 32 ust. 1 rozporządzenia Ministra Finansów regulującego rachunkowość banków. Należy podkreślić, iż tak jak w przypadku treści rozporządzenia zapis ustawy o rachunkowości na przestrzeni ostatnich dekad nie zmieniał się w sposób istotny. Ustawodawca również zachował więc w tym zakresie ciągłość przepisów, z wyjątkiem drobnej korekty semantycznej wskazanej poniżej (różnice wskazano pogrubioną czcionką):

„2. Przy prowadzeniu ksiąg rachunkowych przy użyciu komputera ochrona danych powinna polegać na stosowaniu odpornych na zagrożenia nośników danych, na doborze stosownych środków ochrony zewnętrznej, na systematycznym tworzeniu rezerwowych kopii zbiorów danych **zapisanych na informatycznych nośnikach danych (brzmienie obecnie obowiązujące) / zapisanych na nośnikach komputerowych (brzmienie pierwotne ustawy)**" [ustawa, 1994, art. 71 ust. 2].

Jak widać, korekta wypływała najprawdopodobniej z kwestii technicznego ujęcia poruszanych kwestii oraz postępu technologicznego na przestrzeni ostatnich dekad i nie miała większego wpływu na badaną kwestię. Tyle w zakresie zmian historycznych.

Odnosząc się do kwestii zasadniczych, ustawa w początkowym fragmencie art. 71 stanowi, iż wszelka dokumentacja, księgi rachunkowe, dowody księgowe, dokumenty inwentaryzacyjne oraz sprawozdania finansowe zwane są zbiorami. Ustawodawca wymaga, aby zbiory przechowywać w sposób należyty, chroniąc je przed niedozwolonymi zmianami, które w konsekwencji mogą przyczyniać się do fałszowania lub nieuprawnionych zmian dowodów księgowych. Zabezpieczenia mają na celu także unikanie nieupoważnionego rozpowszechniania, uszkodzenia lub zniszczenia zbiorów [ustawa, 1994, art. 71 ust. 1].

W praktyce bankowej księgi rachunkowe oraz transakcje przeprowadzane są już przy użyciu komputerów. W związku z tym ochrona danych winna polegać m.in. na stosowaniu odpornych na zagrożenia nośników danych, które zabezpieczą je przed zniszczeniem. Kolejnym wymaganym elementem jest zapewnienie adekwatnych środków ochro-

ny zewnętrznej, które mają za zadanie zabezpieczenie przed skutkami zdarzeń losowych, takich jak: kradzieże, zalania, pożary itp. W tym celu wymagane jest systematyczne tworzenie rezerwowych kopii zbiorów danych zapisanych na nośnikach informatycznych. W praktyce tworzone są one codziennie i zabezpieczane w miejscach odległych od głównej siedziby danego podmiotu w celu zapewnienia przestrzennej dywersyfikacji ryzyka.

Kolejnym warunkiem, który stawia ustawa o rachunkowości, jest zapewnienie trwałości zapisu informacji, który umożliwi przechowywanie zbiorów przez czas nie krótszy od wymaganego do przechowywania danego rodzaju ksiąg rachunkowych i dowodów księgowych (będzie o nim mowa nieco później). Wszystkie wymogi mają na celu ochronę wszelkich programów i danych systemu IT w zakresie rachunkowości poprzez stosowanie najwyższej jakości rozwiązań technicznych i organizacyjnych. Nadrzędnym zadaniem w tym zakresie jest ochrona przed nieupoważnionym dostępem lub zniszczeniem spowodowanym zarówno czynnikami wewnętrznymi, jak i zewnętrznymi [ustawa, 1994, art. 71 ust. 1].

Nie mniej istotnym z punktu widzenia weryfikacji problemu badawczego jest zapis art. 74 ustawy o rachunkowości [ustawa, 1994, art. 74 ust. 2 pkt 1–4]. W tym przypadku autor zbadał zarówno brzmienie obowiązujące obecnie, jak i historyczne nowelizacje tego aktu prawnego. W kolejnych nowelizacjach ustawy (aż do chwili obecnej) fragment ten nie uległ zmianie w stosunku do brzmienia pierwotnie analizowanego, z wyjątkiem drobnej korekty (wskazanej poniżej pogrubioną czcionką): „(…) 4) dowody księgowe dotyczące **środków trwałych w budowie** (brzmienie obecnie obowiązujące) / **wieloletnich inwestycji rozpoczętych** (brzmienie pierwotne ustawy)" [ustawa, 1994, art. 74 ust. 2 pkt 4].

Jak widać, podobnie jak w poprzednim przypadku drobnej korekty semantycznej w art. 71 ustawy, zmiana nie miała żadnego wpływu na badaną w niniejszym opracowaniu kwestię, więc można ją pominąć w dalszych rozważaniach.

Wracając do meritum sprawy, należy zaznaczyć, iż postanowienia art. 74 ustawy są rozwinięciem analizowanego uprzednio art. 71. Zawarto tam zapisy, na mocy których zatwierdzone roczne sprawozdania finansowe podlegają tzw. trwałemu przechowywaniu. Oznacza to ni mniej, ni więcej, iż winny być zabezpieczane bezterminowo przez cały okres funkcjonowania danego podmiotu i nie obowiązują w tym zakresie żadne

limity czasowe. Odnośnie do pozostałych dokumentów ustawodawca wyznaczył już ścisłe wymogi przedziałów czasowych przechowywania zbiorów, czego przykładem mogą być księgi rachunkowe, które należy przechowywać przez okres lat pięciu. W praktyce bankowej wiele podmiotów stosuje w swoich procedurach wewnętrznych okresy przekraczające ww. przedział czasowy. Odnośnie do zbiorów wewnętrznych, czyli kart wynagrodzeń pracowników (bądź ich odpowiedników), przez okres wymaganego dostępu do tych informacji, wynikający z przepisów emerytalnych, rentowych oraz podatkowych, nie krócej jednak niż 5 lat.

Istotnym elementem dokumentacji są dowody księgowe dotyczące wpływów ze sprzedaży detalicznej, czyli – w przypadku działalności bankowej – dowody przeprowadzania wszelkiego rodzaju transakcji. W tym zakresie należy je przechowywać do dnia zatwierdzenia sprawozdania finansowego za dany rok obrotowy, ale nie krócej niż do dnia, w którym rozliczono osoby, którym powierzono składniki aktywów objęte daną sprzedażą detaliczną. Może to oznaczać obowiązek przechowywania dokumentacji przez wiele lat w przypadku transakcji długoterminowych.

Kolejny wymóg dotyczy dowodów księgowych obejmujących transakcje pożyczkowe, kredytowe oraz pozostałe umowy handlowe, a także mniej powszechne w sektorze bankowym środki trwałe w budowie w zakresie roszczeń dochodzonych w postępowaniu cywilnym, karnym albo podatkowym. Tutaj ustawodawca wyznaczył okres pięciu lat od początku roku następującego po roku obrotowym, w którym operacje, transakcje i postępowanie zostały ostatecznie zakończone, spłacone, rozliczone lub przedawnione [ustawa, 1994, art. 74 ust. 2]. Zwłaszcza końcowy fragment tego postanowienia jest istotny z punktu widzenia klientów lub kontrahentów banków, którzy wnieśli przeciwko nim sprawy sądowe lub inne roszczenia. W tym zakresie nie są dostępne oficjalne statystyki i zestawienia, niemniej jednak z doświadczenia zawodowego autora niniejszego opracowania wynika, iż w wielu przypadkach okres ten jest błędnie interpretowany zarówno przez podmioty finansowe, jak i klientów. Powodować to może długoterminowe spory, które niejednokrotnie są weryfikowane na drodze sądowej.

3. Ochrona dokumentacji a wymogi Komisji Nadzoru Finansowego

Ze względu na specyfikę sektora bankowego w kontekście problemu badawczego należy uwzględnić również nie mniej ważne akty tzw. miękkiego prawa (Rekomendacje), uchwalane przez organ nadzoru na podstawie zapisów ustawy Prawo bankowe [ustawa, 1997, art. 137 ust. 5], które kształtują w praktyce obowiązujące w bankowości standardy [Sikorski, 2015, s. 362]. Należy zaznaczyć, iż w praktyce rynkowej banki w bardzo dużym stopniu przestrzegają „nieobowiązkowych" zaleceń organu nadzoru, który na mocy nadanych mu uprawnień może w bardzo dotkliwy sposób ukarać podmiot niestosujący się do rekomendacji. Bodaj żaden z zarządów banków działających w Polsce nie przeciwstawił się wprost w ten sposób formułowanym zaleceniom. Zarządy starają się na ogół w możliwie najpełniejszy sposób realizować tego typu oczekiwania rodzimego nadzorcy. Przedstawiciele Komisji Nadzoru Finansowego na oficjalnych spotkaniach na pytania o potencjalne sankcje za nierealizowanie „nieobowiązkowych" przecież rekomendacji odpowiadają najczęściej, iż w takich przypadkach bank musi wykazać i skutecznie przekonać organ nadzoru, iż jego zalecenia nie są zasadne i w przypadku danego banku nie mogą być z jakiegoś względu wdrożone. W niemal wszystkich przypadkach tego typu proces skończyłby się prawdopodobnie niepowodzeniem. Organ nadzoru realizuje kontrole w instytucjach bankowych, które kończą się tzw. zaleceniami pokontrolnymi. Na ich mocy bank byłby już zobligowany do realizacji wskazanych w rekomendacjach czynności. Nadto w praktyce rynkowej członkowie zarządów unikają konfliktów z organem nadzoru, który na mocy ustawy wyraża zgodę m.in. na objęcie funkcji prezesa lub członka zarządu banku. Nikt z urzędujących członków zarządu nie będzie ryzykował konfliktu z nadzorcą i podejmował długoterminowego ryzyka niewyrażenia zgody w przypadku zmiany miejsca pracy i chęci zasiadania w zarządzie innego banku lub instytucji finansowej. Powyższy wywód ma na celu wskazanie, iż z różnych względów banki przywiązują bardzo dużą wagę do tego typu aktów prawnych (o tzw. miękkiej naturze) i w praktyce ich postanowienia są bardzo skrupulatnie realizowane.

Poniżej wyszczególniono główne akty uchwalane przez organ nadzoru, które zawierają postanowienia w zakresie bezpieczeństwa i ochrony dokumentacji bankowej. Zapisy dotyczące ww. kwestii zawierały się niejednokrotnie w rekomendacjach i uchwałach dotyczących kontroli

wewnętrznej oraz zarządzania ryzykiem. Ryzyko w tym przypadku należy rozumieć także jako ryzyko i bezpieczeństwo informatyczne, ponieważ większość dokumentacji sektora bankowego jest gromadzona i archiwizowana właśnie w tej formie. W ujęciu chronologicznym należy zaliczyć do ww. regulacji następujące dokumenty:

1) Rekomendacja D – dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki, Komisja Nadzoru Bankowego Generalny Inspektorat Nadzoru Bankowego, Narodowy Bank Polski, Warszawa, 1997 r.
2) Rekomendacja H – dotycząca kontroli wewnętrznej w banku, Komisja Nadzoru Bankowego Generalny Inspektorat Nadzoru Bankowego, Narodowy Bank Polski, Warszawa, 1999 r.
3) Rekomendacja D – dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki, Komisja Nadzoru Bankowego Generalny Inspektorat Nadzoru Bankowego, Narodowy Bank Polski, Warszawa, 2002 r.
4) Rekomendacja H – dotycząca kontroli wewnętrznej w banku, Komisja Nadzoru Bankowego Generalny Inspektorat Nadzoru Bankowego, Narodowy Bank Polski, Warszawa, 2002 r.
5) Rekomendacja M – dotycząca zarządzania ryzykiem operacyjnym w bankach, Komisja Nadzoru Bankowego Generalny Inspektorat Nadzoru Bankowego, Narodowy Bank Polski, Warszawa, 2004 r.
6) Uchwała Nr 4/2007 Komisji Nadzoru Bankowego z dnia 13 marca 2007 r. w sprawie szczegółowych zasad funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz szczegółowych warunków szacowania przez banki kapitału wewnętrznego i dokonywania przeglądów procesu szacowania i utrzymywania kapitału wewnętrznego.
7) Uchwała Nr 383/2007 Komisji Nadzoru Finansowego z dnia 17 grudnia 2008 r. w sprawie szczegółowych zasad funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz szczegółowych warunków szacowania przez banki kapitału wewnętrznego i dokonywania przeglądów procesu szacowania i utrzymywania kapitału wewnętrznego.
8) Rekomendacja H – dotycząca systemu kontroli wewnętrznej w bankach, Komisja Nadzoru Finansowego, Warszawa, 2011 r.
9) Uchwała Nr 258/2011 Komisji Nadzoru Finansowego z dnia 4 października 2011 r. w sprawie szczegółowych zasad funkcjonowania

systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz szczegółowych warunków szacowania przez banki kapitału wewnętrznego i dokonywania przeglądów procesu szacowania i utrzymywania kapitału wewnętrznego oraz zasad ustalania polityki zmiennych składników wynagrodzeń osób zajmujących stanowiska kierownicze w banku.

10) Rekomendacja D – dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, Komisja Nadzoru Finansowego, Warszawa, styczeń 2013 r.
11) Rekomendacja M – dotycząca zarządzania ryzykiem operacyjnym w bankach, Komisja Nadzoru Finansowego, Warszawa, styczeń 2013 r.

Każdy z ww. dokumentów w nieco inny sposób ujmuje i reguluje kwestie tworzenia, przechowywania i ochrony dokumentacji bankowej. Treść ich wskazuje, jak rodzimy nadzorca dostosowywał wymogi do zmieniającego się rynku i nowych wyzwań technologicznych. Historyczna obserwacja treści wszystkich dokumentów ze względu na ograniczone ramy niniejszej publikacji może być przeprowadzona w odrębnym opracowaniu. Niemniej jednak jako przykład niech posłuży Rekomendacja D, która reguluje zarządzanie obszarami ryzyka związanymi ze stosowaniem technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach. Jak wynika z wcześniejszego zestawienia, dokument był publikowany przez organ nadzoru trzykrotnie. Banki zawsze były, są i będą narażone na ryzyko błędów i oszustw, ale skala i szybkość, z jaką mogą one występować, zwiększa się wraz ze wzrostem skali przepływu środków pieniężnych na rynkach globalnych. Rodzaje ryzyk występujące w systemach informatycznych i w bankowości elektronicznej są szersze niż w ukształtowanych wcześniej strukturach bankowych opartych na systemach klasycznych (na papierowej ewidencji danych). W porównaniu z systemami wcześniejszymi w systemie elektronicznego przetwarzania danych szczególne ryzyko rodzi możliwość bezprawnego ujawnienia, modyfikacji lub usunięcia znacznej ilości informacji. Możliwe jest to do zrealizowania w bardziej dogodny i metodologicznie dostępny sposób (np. kopie na nośnikach danych) bez pozostawienia śladów nieautoryzowanego dostępu.

Szczególnej uwagi wymaga także zagadnienie zapewnienia właściwej i bezpiecznej dostępności do tego typu systemów. Zarządzanie ryzykiem towarzyszącym systemom informatycznym i telekomunikacyjnym w rekomendacji zostało podzielone na cztery ogólne zagadnienia: rola

kierownictwa banku w zarządzaniu bezpieczeństwem systemów informatycznych, mechanizmy kontroli bezpieczeństwa, zarządzanie ryzykami oraz audyt informatyczny i nadzór. Jeden z kluczowych elementów rekomendacji dotyczy procedur postępowania i ostrożności w zakresie dostępu do systemów bankowych w celu uniknięcia nadużyć w zakresie potwierdzania tożsamości klientów. Komisja rekomenduje, aby bazy danych dotyczące tożsamości, zapewniające dostęp do rachunków, były należycie chronione przed wszelkimi manipulacjami oraz korupcją. Wskazuje się tym samym także na czynniki wewnętrzne, czyli możliwe nadużycia uprawnień przez pracowników banków. Wszelkie próby manipulacji winny być systemowo wykrywalne, a nadto powinny istnieć tzw. ścieżki audytu umożliwiające udokumentowanie wszelkich takiego rodzaju prób. Powyższe mechanizmy powinny umożliwiać identyfikację każdego przypadku dodania, usunięcia lub zmiany danych poprzez transparentne mechanizmy autoryzacji [Rekomendacja D, 2002, s. 21, 24].

Rekomendacja wskazuje, iż nikt z pracowników lub współpracowników banku nie powinien mieć uprawnień lub przywilejów dostępu do baz danych bez należytej autoryzacji, nawet w przypadku tzw. administratorów systemów. W tym zakresie wskazano na obowiązek bardziej surowych wewnętrznych mechanizmów kontroli oraz podziału obowiązków w zespołach administratorów. Dodatkowym elementem są postulaty w zakresie mechanizmów uodpornienia baz danych na manipulacje dzięki procesowi stałego ich monitorowania. Jednym z mechanizmów zabezpieczających a zarazem umożliwiających identyfikację niepożądanych zjawisk w powyższym zakresie jest obowiązek tworzenia w bankach komórek kontroli wewnętrznej odpowiedzialnych m.in. za audyty systemów informatycznych. W tym zakresie wymagane są wszelkiego rodzaju pisemne procedury zabezpieczania i zarządzania bezpieczeństwem systemów IT oraz innych aktywności banków. Mają one zapewnić ciągłość i bezpieczeństwo funkcjonowania każdego z elementów systemu, jak i umożliwiać retrospektywne analizy, których zadaniem jest identyfikacja nadużyć na wszystkich szczeblach działalności danego podmiotu [Rekomendacja D, 2002, s. 21, 24]. Pozostałe elementy rekomendacji również podporządkowane są jednemu celowi nadrzędnemu – zapewnieniu maksymalnego poziomu bezpieczeństwa systemów oraz ewidencjonowanej w nich dokumentacji będącej podstawą przeprowadzanych transakcji bankowych.

Zakończenie

Podsumowując powyższe rozważania, należy stwierdzić, iż specyfika pojęcia „dokumentacja bankowa" w ostatnich dekadach znacznie ewoluowała i obejmuje obecnie przede wszystkim dokumenty w formie elektronicznej. Ze względu na skalę funkcjonowania, wzrost liczby i tempa transakcji oraz globalizację rynków klasyczna, papierowa forma dokumentowania transakcji byłaby nieefektywna, a wręcz uniemożliwiałaby sprawną ich realizację [Zawadzka, 2003, s. 421–428]. To z kolei skutkuje pojawieniem się szeregu nowych ryzyk właściwych dla elektronicznej formy ewidencjonowania i realizowania transakcji bankowych. Wyzwania w tym zakresie wzrastają wraz z rozwojem rynku, a tym samym banki muszą im sprostać, tak aby nie zagroziły płynnemu funkcjonowaniu pojedynczych podmiotów oraz całego systemu finansowego.

Podstawą w tym zakresie są analizowane w niniejszym opracowaniu regulacje i ich ewolucja. W rodzimym systemie bankowym regulacje dotyczące tworzenia, przechowywania i ochrony dokumentacji funkcjonują na kilku płaszczyznach. Tym samym w pierwszej kolejności uwaga skupiona została na analizie głównego aktu prawnego regulującego sektor, czyli ustawie Prawo bankowe, gdzie zawarto główne zasady dotyczące tego zakresu działalności bankowej. Badanie wykazało, iż ustawa ta wyznacza jedynie ogólne ramy i obowiązki banków dotyczące gromadzenia i ochrony dokumentacji, a szczegółowe kwestie delegowane są do innych aktów prawnych w formie rozporządzeń. Następnie badaniu poddano przepisy dotyczące rachunkowości banków. W tym zakresie skonfrontowano stosowne rozporządzenie Ministra Finansów regulujące ten obszar aktywności banków, które w kwestiach kluczowych wskazuje szereg wymogów zdefiniowanych szczegółowo w nadrzędnym akcie prawnym, czyli ustawie o rachunkowości. Tak więc banki w kluczowych kwestiach dotyczących gromadzenia, przechowywania i ochrony dokumentacji traktowane są podobnie jak inne podmioty gospodarcze. Przykładem może być tutaj ustawowy obowiązek dotyczący terminów przechowywania zbiorów w zależności od ich specyfiki i rodzajów. Na tym tle szczególne znaczenie mają najbardziej szczegółowe wymogi, które zawarte są w rekomendacjach wydawanych przez Komisję Nadzoru Finansowego. Ze swej natury organ nadzoru na mocy przysługujących mu uprawnień wskazanych w ustawie Prawo bankowe może wskazywać i sugerować rozwiązania, które skutkować mają maksymalizacją bezpieczeństwa i ochroną interesów banków oraz klientów. KNF wykazywał w tym

zakresie dużą aktywność, uchwalając na przestrzeni ostatnich lat rekomendacje dotyczące różnych obszarów aktywności banków oraz dokonując ich kolejnych nowelizacji. Zwłaszcza ten ostatni aspekt pokazuje, jak szybko postęp technologiczny i rozwój rynków globalnych skutkuje powstawaniem nowych ryzyk i zagrożeń, które winny być należycie identyfikowane i antycypowane.

Podsumowując rozważania wynikające z podjętych badań, należy stwierdzić, iż rodzimy system bankowy posiada należyte podstawy regulacyjne w zakresie tworzenia, przechowywania i zabezpieczania dokumentacji. Winny one skutkować w praktyce należytą ochroną i zabezpieczeniem interesu klientów. Niemniej jednak podstawy formalnoprawne i zapisy zawarte w poszczególnych dokumentach są jedynie wskazaniami i wytycznymi, które winny być przestrzegane i realizowane przez poszczególne podmioty. Nowe wyzwania technologiczne, wzrost konkurencji oraz wspomniana wcześniej globalizacja stawiają w tym zakresie coraz wyższe wymagania [Garczyński, 2003, s. 88–89]. To z kolei skutkuje systematycznym wzrostem kosztów ponoszonych przez banki na rozwój systemów oraz ich zabezpieczanie. Ten element jednak będzie już immanentną cechą towarzyszącą bankom oraz innym instytucjom finansowym w przyszłości. Należy domniemywać tym samym, iż nowe wyzwania w tym zakresie skutkować będą kolejnymi nowelizacjami i zmianami w treści regulacji dotyczących omawianej w niniejszym opracowaniu kwestii tworzenia, przechowywania i zabezpieczania dokumentacji bankowej.

Literatura

1. Garczyński D. (2003), *Produkty i usługi bankowości elektronicznej w kontekście globalizacji rynków finansowych*, w: *Bankowość wobec procesów globalizacji*, Pawłowicz L., Wierzba R. (red.), CeDeWu, Warszawa.
2. Krzyżkiewicz Z. (2008), *Bankowość – Podręcznik akademicki*, Jaworski W. L., Zawadzka Z. (red.), Poltekst, Warszawa.
3. Rekomendacja D – dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (2013), Komisja Nadzoru Finansowego, Warszawa.
4. Rekomendacja D – dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki (1997), Komisja Nadzoru Bankowego Generalny Inspektorat Nadzoru Bankowego, Narodowy Bank Polski, Warszawa.

5. Rekomendacja D – dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki (2002), Komisja Nadzoru Bankowego Generalny Inspektorat Nadzoru Bankowego, Narodowy Bank Polski, Warszawa.
6. Rekomendacja H – dotycząca kontroli wewnętrznej w banku (1999), Komisja Nadzoru Bankowego Generalny Inspektorat Nadzoru Bankowego, Narodowy Bank Polski, Warszawa.
7. Rekomendacja H – dotycząca kontroli wewnętrznej w banku (2002), Komisja Nadzoru Bankowego Generalny Inspektorat Nadzoru Bankowego, Narodowy Bank Polski, Warszawa.
8. Rekomendacja H – dotycząca systemu kontroli wewnętrznej w bankach (2011), Komisja Nadzoru Finansowego, Warszawa.
9. Rekomendacja M – dotycząca zarządzania ryzykiem operacyjnym w bankach (2004), Komisja Nadzoru Bankowego Generalny Inspektorat Nadzoru Bankowego, Narodowy Bank Polski, Warszawa.
10. Rekomendacja M – dotycząca zarządzania ryzykiem operacyjnym w bankach (2013), Komisja Nadzoru Finansowego, Warszawa.
11. Rozporządzenia Ministra Finansów z dnia 1 października 2010 r., t.j. Dz.U. z 2013 r. poz. 329.
12. Rozporządzenie Ministra Finansów z dnia 10 grudnia 2001 r. w sprawie szczególnych zasad rachunkowości banków, Dz.U. Nr 149, poz. 1673.
13. Rozporządzenie Ministra Finansów z dnia 29 sierpnia 2008 r. w sprawie szczególnych zasad rachunkowości banków, Dz.U. Nr 161, poz. 1002.
14. Rozporządzenie Ministra Sprawiedliwości z dnia 27 września 2004 r. w sprawie warunków i trybu umarzania dokumentów potwierdzających zawarcie umowy rachunku oszczędnościowego oraz rachunku terminowej lokaty oszczędnościowej, Dz.U. Nr 222, poz. 2258.
15. Rozporządzenie Rady Ministrów z dnia 25 lutego 2003 r. w sprawie zasad tworzenia, utrwalania, przechowywania i zabezpieczania, w tym przy zastosowaniu podpisu elektronicznego, dokumentów bankowych sporządzanych na elektronicznych nośnikach informacji, Dz.U. Nr 51, poz. 442.
16. Sikorski G. (2015), *Prawo bankowe – komentarz*, C.H. Beck, Warszawa.
17. Smyczek S (2012), *Nowe trendy w zachowaniach konsumentów na rynkach finansowych*, Placet, Warszawa.

18. Uchwała Nr 258/2011 Komisji Nadzoru Finansowego z dnia 4 października 2011 r. w sprawie szczegółowych zasad funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz szczegółowych warunków szacowania przez banki kapitału wewnętrznego i dokonywania przeglądów procesu szacowania i utrzymywania kapitału wewnętrznego oraz zasad ustalania polityki zmiennych składników wynagrodzeń osób zajmujących stanowiska kierownicze w banku.
19. Uchwała Nr 383/2007 Komisji Nadzoru Finansowego z dnia 17 grudnia 2008 r. w sprawie szczegółowych zasad funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz szczegółowych warunków szacowania przez banki kapitału wewnętrznego i dokonywania przeglądów procesu szacowania i utrzymywania kapitału wewnętrznego.
20. Uchwała Nr 4/2007 Komisji Nadzoru Bankowego z dnia 13 marca 2007 r. w sprawie szczegółowych zasad funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz szczegółowych warunków szacowania przez banki kapitału wewnętrznego i dokonywania przeglądów procesu szacowania i utrzymywania kapitału wewnętrznego.
21. Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego, t.j. Dz.U. z 2016 r. poz. 1822, z późn. zm.
22. Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe, t.j. Dz.U. z 2016 r. poz. 1988 z późn. zm.
23. Ustawa z dnia 29 września 1994 r. o rachunkowości, t.j. Dz.U. z 2016 r. poz. 1047 z późn. zm.
24. Zawadzka Z. (2003), *Globalizacja a sektor bankowy w Polsce*, w: Bankowość wobec procesów globalizacji, Pawłowicz L., Wierzba R. (red.), CeDeWu, Warszawa.

Streszczenie

Celem niniejszego opracowania jest analiza adekwatności wymogów i regulacji w zakresie tworzenia, przechowywania i zabezpieczania dokumentów bankowych w kontekście ochrony interesu klientów. Uwaga skupiona została na rynku krajowym, a zakres analizy objął zarówno obecne, jak i historyczne brzmienia dokumentów formalnoprawnych wiążących rodzime banki w wyżej wskazanym zakresie. Regulacje dotyczące tworzenia, przechowywania i ochrony dokumentacji funkcjonują na kilku płaszczyznach. Analizie poddano zapisy ustawy Prawo bankowe, w której zawarto pryncypia dotyczące tego zakresu

działalności bankowej. Następnie badaniu poddano przepisy dotyczące rachunkowości banków. W tym zakresie skonfrontowano stosowne rozporządzenie Ministra Finansów regulujące ten obszar aktywności banków, które w kwestiach kluczowych wskazuje szereg wymogów zdefiniowanych szczegółowo w nadrzędnym akcie prawnym, czyli ustawie o rachunkowości. Na tym tle szczególne znaczenie mają najbardziej szczegółowe wymogi, które zawarte są w rekomendacjach wydawanych przez Komisję Nadzoru Finansowego. Zapisy aktów prawnych i ich zmiany pokazują, jak szybko postęp technologiczny i rozwój rynków globalnych skutkuje powstawaniem nowych ryzyk i zagrożeń, które winny być należycie identyfikowane i antycypowane. Powyższe zagadnienia ujęto w trzech kolejnych częściach artykułu opisujących najważniejsze elementy i szczegóły przeprowadzonych badań.

Słowa kluczowe
bank, dokumentacja, zbiory, rekomendacje, bezpieczeństwo

Requirements and regulations' analysis for creation, storage and bank documents protection in the context of customers' interest (Summary)

The aim of this study is to analyze the adequacy of requirements and re-regulation for creation, storage and bank documents protection in the context of customers' interest. The scope of the analysis took both current and historical versions of formal and legal documents. Regulations concerning for creation, storage and bank documents protection operate on several levels. We analyzed the provisions of the Banking Law, which contains the main principles concerning the banking activities. Then the study were subjected provisions concerning bank accounting rules: the Minister of Finance act and the Accounting Act. Very important are the most specific requirements of recommendations issued by the Financial Supervision Commission. These issues included in the next three parts describe the most important elements and details of the analysis.

Keywords
bank, documentation, storage, recommendations, protection