ISSN 1429-2939

Nr 3(68) 2017

BEZPIECZNY BANK

BFG

BANKOWY FUNDUSZ GWARANCYJNY

BEZPIECZNY BANK jest czasopismem wydawanym przez Bankowy Fundusz Gwarancyjny od 1997 roku, poświęconym zagadnieniom stabilności systemu finansowego, ze szczególnym uwzględnieniem systemu bankowego.

Artykuły publikowane w BEZPIECZNYM BANKU są recenzowane.

Za publikację naukową w BEZPIECZNYM BANKU Minister Nauki i Szkolnictwa Wyższego przyznał trzynaście punktów.

Pismo BEZPIECZNY BANK wydawane jest wyłącznie w wersji elektronicznej – **www.bfg.pl**.

REDAKCJA:
Krystyna Kawerska

WYDAWCA:
Bankowy Fundusz Gwarancyjny
ul. Ks. Ignacego Jana Skorupki 4
00-546 Warszawa

SEKRETARIAT REDAKCJI:
Ewa Teleżyńska, Małgorzata Polak
Telefon: 22 583 08 78, 22 583 05 74
e-mail: ewa.telezynska@bfg.pl; malgorzata.polak@bfg.pl

Informacje dotyczące wymogów formalnych i edytorskich dla autorów publikacji znajdują się na stronie: www.bfg.pl

DOM WYDAWNICZY ELIPSA

Opracowanie komputerowe, druk i oprawa:
Dom Wydawniczy ELIPSA
ul. Inflancka 15/198, 00-189 Warszawa
tel./fax 22 635 03 01, 22 635 17 85
e-mail: elipsa@elipsa.pl, www.elipsa.pl

Bezpieczny Bank
3(68)/2017

DOI: 10.26354/bb.7.3.68.2017

Stanisław Kasiewicz*
Lech Kurkliński**

RYZYKO KLIENTA I KULTURA RYZYKA A ROZWÓJ BANKOWOŚCI CYFROWEJ

1. WSTĘP

Rynek usług finansowych i pozycja instytucji na nim funkcjonujących dość istotnie różnią się w stosunku do innych branż. W szczególności dotyczy to przewagi jaką uzyskują one wobec swoich klientów z tytułu asymetrii informacji. Wynika ona m.in. z dysproporcji w wiedzy na temat finansów, a także prawa obowiązującego w tej dziedzinie. Sytuacja o podobnym charakterze występuje także w innych obszarach obrotu gospodarczego na linii klient (zwłaszcza konsument) a usługodawca. Jednakże szczególnie relacje te, jeśli chodzi o banki, dodatkowo oceniane są poprzez pryzmat traktowania ich jako instytucji zaufania publicznego. Dlatego też przypadki naruszenia zasad etycznego postępowania są poddawane powszechnej krytyce. Nakładają się na to inne czynniki o charakterze kulturowym i ekonomicznym (uprzywilejowana pozycja z tytułu regulacji, licencjonowanie dostępu, siła finansowa, podmioty szczególnej troski władz publicznych – „zbyt duże i ważne, aby upaść", wysokie wynagrodzenia itd.), które wyróżniają banki na tle innych podmiotów. Na powyższe aspekty

* Prof. zw. dr hab. Stanisław Kasiewicz jest sekretarzem naukowym ALTERUM Ośrodka Badań i Analiz Systemu Finansowego oraz pracownikiem Zakładu Zarządzania Ryzykiem Instytutu Finansów Korporacji i Inwestycji, Kolegium Nauk o Przedsiębiorstwie Szkoły Głównej Handlowej w Warszawie.

** Dr hab. Lech Kurkliński jest dyrektorem ALTERUM Ośrodka Badań i Analiz Systemu Finansowego oraz pracownikiem Zakładu Zarządzania Ryzykiem Instytutu Finansów Korporacji i Inwestycji, Kolegium Nauk o Przedsiębiorstwie Szkoły Głównej Handlowej w Warszawie.

zwrócono szczególną uwagę w kontekście ostatniego globalnego kryzysu finansowego i społecznej percepcji środowiska bankowego[1]. Dużo publikacji podkreśla, że przez dziesięciolecia kultura była ignorowana jako źródło ryzyka bankowego i stabilności sektora bankowego. Po 2008 r. w zarządzaniu ryzykiem szerzej dostrzeżono liczne słabości m.in.: nadmierne zaufanie zarządów banków do wyników zawansowanych modeli pomiaru ryzyka, słaby system komunikacji wewnątrz banków, chciwość bankowców, nieprzestrzeganie podstawowych norm etycznych, brak odpowiedzialności pracowników na niższych szczeblach za zarządzanie ryzykiem.

Jednakże w ostatnich latach nasilił się także inny czynnik sprawczy, który skłania, aby na nowo analizować pozycję klienta korzystającego z usług bankowych, a mianowicie zmiany technologiczne. W szczególności skutki cyfryzacji wywołują potrzebę odmiennego definiowania relacji bank – klient, wymuszając zmiany modeli biznesowych wobec nowych uwarunkowań konkurencji na rynku bankowym. Często powodują one, że złożone innowacje finansowe adresowane są do klientów o bardzo niskiej wiedzy finansowej. Coraz ważniejszym problemem społecznym staje się wykluczenie finansowe relatywnie dużych grup potencjalnych klientów. W związku z tym zmienia się system europejskich regulacji banków w zakresie ochrony klientów. Tę politykę czytelnie prezentuje J. Monkiewicz. Uznaje, że nowy paradygmat regulacyjny ochrony konsumentów na rynkach finansowych[2]:

- odrzuca hipotezę mądrych i racjonalnych wyborów konsumenta i podkreśla rolę determinant behawioralnych,
- kwestionuje faktyczną przydatność tylko formalnych wymogów przejrzystości oferty bankowej jako skutecznych narzędzi ochrony konsumenta,
- akcentuje potrzebę rozwoju wyspecjalizowanych instytucji ochrony konsumentów, które winny być częścią całościowego podejścia nadzorczego.

Wobec powyższych uwag należy porównać ryzyko klienta w tradycyjnym modelu bankowości z zagrożeniami, jakie już się pojawiają lub mogą wystąpić w dobie cyfryzacji. Szczególną rolę przypisuje się uwarunkowaniom kulturowym niezbędnym dla przeprowadzenia transformacji banków do działania w nowych warunkach. Jednakże wcześniej konieczne jest określenie różnic w istocie i w podejściu do ryzyka klienta cyfrowego w stosunku do dotychczas dominujących zasad i narzędzi

---

1 W. Dudley, *Enhancing Financial Stability by Improving Culture in the Financial Services Industry.* Remarks at The Workshop on Reforming Culture and Behavior in the Financial Services Industry, Federal Reserve Bank of New York, October 20, 2014; Group of Thirty, *Banking Conduct and Culture: A Call for Sustained and Comprehensive Reform*. Monograph, Washington, D.C., July 2015; S. Ochs, *Inside the Banker's Brain: Mental Models in the Financial Services Industry and Implications for Consumers*, *Practitioners and Regulators*, Monograph, Initiative on Financial Security, The Aspen Institute, 2014.

2 J. Monkiewicz, *W poszukiwaniu nowego paradygmatu ochrony konsumentów na rynkach finansowych*. Referat na konferencję *Jak chronić konsumenta na rynku finansowym? Modele i doświadczenia międzynarodowe,* Rzecznik Finansowy, Warszawa 11.10.2017.

zarządzania ryzykiem bankowym. Sytuacja ta prowadzi do potrzeby stworzenia nowej klasyfikacji ryzyka klienta, uwzględniającej kulturowe uwarunkowania, ale jednak głównie przez pryzmat innowacji technologicznych. Omawiana problematyka przedstawiana jest na tle polskiego rynku usług bankowych, który w stosunku do innych krajów UE cechuje się nie tylko stabilnością, bezpieczeństwem, ale również właśnie wysoką innowacyjnością.

1. OCENA AKTUALNEJ POZYCJI KLIENTA W RELACJACH Z BANKAMI

W tradycyjnym podejściu do konkurencji rynkowej zwraca się uwagę na następujące kryteria[3]:

a) bariery wejścia i wyjścia na rynek,
b) liczbę podmiotów i ich udziały rynkowe,
c) zróżnicowanie oferowanych produktów (usług),
d) koszty poszukiwania dostawców przez odbiorców,
e) preferencje odbiorców.

W przypadku sektora bankowego zachodzą obecnie istotne zmiany w odniesieniu do każdego z wymienionych przekrojów. Jeśli chodzi o bariery wejścia, to nadal obowiązuje wymóg uzyskania licencji bankowej, zamykający krąg dostawców usług. Jednakże otwarcie na fin-techy oraz inne podmioty ze sfery *shadow bankingu* łamie te oligopolistyczne cechy rynku bankowego. Przeobrażenia zachodzą też w odniesieniu do liczby podmiotów. Tutaj z jednej strony następuje konsolidacja banków (eliminowanie mniejszych podmiotów, głównie przez fuzje i przejęcia, a także rzadko powstają nowe), ale pojawiają się inni niebankowi konkurenci, oferujący podobne, a nawet takie same usługi. Do tej pory stosunkowa łatwość kopiowania usług bankowych i inercja banków kreowały duży stopień homogeniczności tego rynku, co najmniej pod kątem produktowym. Aczkolwiek i tu nowi gracze w postaci instytucji oficjalnie nie będących bankami istotnie zaczęli zmieniać oblicze różnorodności oferty dla klientów, m.in. ze względu na ich zwinność, elastyczność, innowacyjność, proponowanie prostych i wygodnych usług itd. oraz przenoszenie walki konkurencyjnej głównie do sfery cyfrowej. Właśnie z tego powodu następuje rewolucja w formach poszukiwania dostawców przez odbiorców i presja na obniżkę kosztów. Wspomniana na wstępie asymetria informacyjna powoli wyrównuje się (internet otworzył ogromne możliwości dostępu do informacji, dokonywania porównań, zbierania opinii etc.) i powraca zainteresowanie suwerennością konsumenta. Oprócz aspektów technologicznych kryzys finansowy bardzo silnie wzmocnił aktywność klientowską, ośmieloną falą krytyki sektora bankowego. Niewątpliwie za-

[3] P. Maciąg, *Wirtualna a doskonała konkurencja*, "E-mentor", 2016, nr 5(67).

sadniczym zmianom ulegają preferencje odbiorców z uwagi na przenoszenie coraz to nowych aktywności do cyberprzestrzeni, zmiany globalizacyjne, cywilizacyjne i demograficzne[4]. Dotyczy to zarówno kształtowania się postaw klientów, jak i coraz szerszych możliwości wykorzystania informacji o nich w ramach tzw. Big Data.

Zachodzące zmiany nie oznaczają, że stare problemy w relacjach bank – klient znikają. Cały czas newralgiczne pozostają kwestie nierespektowania obowiązujących praw. Wiążą się one głównie z:

a) adhezyjnym narzucaniem przez banki niekorzystnych dla klientów umów, włącznie z wprowadzaniem do nich klauzul, uważanych za abuzywne,
b) ukrywaniem rzeczywistych kosztów (oprocentowania, opłat, prowizji, spreadów walutowych itd.),
c) zjawiskiem missellingu, czyli świadomej sprzedaży produktów niedostosowanych do aktualnych potrzeb klientów,
d) nieinformowaniem o faktycznych rodzajach i natężeniu ryzyka związanego z danym produktem,
e) nieuwzględnianiem praw do reklamacji i ich niekorzystnym dla klientów rozpatrywaniem,
f) stosowaniem nieuczciwej reklamy.

Do tych dotychczasowych potrzeb zwiększonej ochrony klientów banków dochodzą nowe wyzwania związane z jednej strony ze zmieniającą się pozycją i charakterystyką odbiorców usług finansowych, a z drugiej zupełnie nowymi rodzajami ryzyka wynikającymi z cyberzagrożeń.

Nowy model bankowego cyber klienta coraz bardziej zbliża się do kogoś, kto potrzebuje inteligentnych usług finansowych, które mają być wsparciem konkretnych potrzeb konsumpcyjnych i to w jak najmniej absorbujący sposób (konsumeryzacja bankowości). Postęp w tej dziedzinie jest ogromny (wygoda, dostępność i personalizacja usług detalicznych, sztuczna inteligencja, biometria, geolokalizacja itd.), choć jeszcze mocno fragmentaryczny[5]. Jednakże, aby instytucje finansowe działały w sposób kompleksowy, powinny całościowo zmienić swój model biznesowy, a w tym podejście kulturowe (m.in. wywołane zmianami demograficznymi). Banki zmuszone są do odchodzenia od koncentracji uwagi na doskonaleniu funkcji operacyjnych (aczkolwiek cały czas bardzo ważnych), gdzie technologia pozwoliła na znaczący spadek kosztów operacyjnych i wzrost efektywności. Polem walki konkurencyjnej stają się relacje z klientami, z wykorzystaniem innowacji do ich pozyskiwania oraz utrzymywania. Ważnym krokiem, aby podejmować rozsądne i uzasadnione działania budujące zaufanie klientów, jest poznanie i kształtowanie kultury ryzyka banku jako instytucji.

---

4 *Managing change and risk in the age of digital transformation. The digital journey of financial institutions in ASEAN*, E&Y Report, Singapore 2016.

5 *Ibidem.*

2. KULTURA RYZYKA

Kultura ryzyka jest pojęciem, które poddaje się z trudnością jednoznacznej definicji, interpretacji i badaniu, choćby z tego powodu, że składa się z dwóch wysoce pojemnych, złożonych, wielowymiarowych kategorii, tj. kultury oraz ryzyka. Najprościej można ją zdefiniować jako wspólne wartości, postawy i zachowania podzielane w banku, które pozwalają głębiej i szerzej zrozumieć, identyfikować i zarządzać ryzykiem[6]. Genezy badań nad kulturą ryzyka nie jest łatwo odnaleźć. Ważniejsze wydaje się jednak wzrastające zainteresowanie jej rolą, koncepcjami i analizami. Ten dynamiczny wzrost, zwłaszcza po rozpoczęciu kryzysu finansowego, ilustrują statystyki poszukiwań frazy „kultura ryzyka" w internecie – przyrost o charakterze wykładniczym[7]. Nie tylko akademicy zainteresowali się tą problematyką, ale także praktycy, w tym szczególnie firmy konsultingowe (np. Deloitte, McKinsey, PWC) oraz organy nadzorcze.

Problematyka kultury ryzyka pojawiła się w pracach Komitetu Europejskich Nadzorców Bankowych (*Committee of European Banking Supervisors* CEBS). Wytyczne w tej dziedzinie zawarto w „Głównych zasadach zarządzania ryzykiem" (*High level principles for risk management*)[8]. Przyjęte wytyczne dotyczyły wielu aspektów funkcjonowania banków, ale w kontekście ryzyka cyfrowego na uwagę zasługuje zwrócenie uwagi na rolę każdego członka organizacji, który musi być w pełni świadomy swoich obowiązków związanych z identyfikacją i raportowaniem istotnych rodzajów ryzyka. Kultura ryzyka powinna być w polu zainteresowania nie tylko kierownictwa, ale i szeregowych pracowników we wszystkich jednostkach organizacji i dotyczyć każdego ważnego aspektu ryzyka (nie tylko finansowego, ale np. ryzyka operacyjnego, reputacji). Ponadto nowe uwarunkowania wymuszają posiadanie spójnej i silnej kultury ryzyka, wyrażonej w rzetelnych (formalnych i co jest równie ważne – nieformalnych) zasadach zarządzania ryzykiem, wspomaganych przez odpowiednią politykę komunikacyjną, dostosowaną do wielkości, złożoności i zmienności organizacji oraz profilu ryzyka danego podmiotu (grupy kapitałowej).

W podobny sposób wypowiedział się *Financial Stability Board* (FSB). W dokumencie wydanym w 2014 r. wskazano na cztery grupy zagadnień[9]:

---

6 *Risk Culture*. Institute of Risk Management. October 2012, s. 7.

7 M. Power, S. Ashby, T. Palermo, *Risk Culture in Financial Organizations: Final Report*, Financial Services Knowledge Transfer Network, London 2013, www.lse.ac.uk/researchAndExpertise/units/CARR/pdf/Final (dostęp: 14.04.2017).

8 *High level principles for risk management*, Committee of European Banking Supervisors, London, 2014, https://www.eba.europa.eu/documents/10180/16094/HighLevelprinciplesonriskmanagement.pdf (dostęp: 15.03. 2017).

9 *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture. A Framework for Assessing Risk Culture*, Financial Stability Board,7 April 2014.

1) wyznaczanie podstawowych wartości i zasad jakie powinny obowiązywać w instytucjach finansowych, włącznie z systemami ich monitorowania i kontroli;
2) odpowiedzialność zarówno pracowników, jak i kadry kierowniczej za percepcję ryzyka, podejmowane działania i przestrzeganie ustalonych wartości oraz zasad;
3) poprawa komunikacji (otwartości i skuteczności) oraz tworzenie pozytywnego klimatu dla wymiany poglądów, testowanie nowych praktyk i zachęcanie do współpracy między pracownikami;
4) systemy motywacyjne (finansowe i pozafinansowe) sprzyjające wdrażaniu holistycznego podejścia do kultury ryzyka, zrywającego z ujęciem silosowym.

Szczególnie pod kątem ryzyka cyfrowego znaczenie ma:

a) wykrywanie (identyfikowanie), ocena i redukowanie ryzyka w taki sposób, że stanowi to codzienną część pracy każdego z pracowników, dlatego też musi to być zakodowane jako stały nawyk,
b) akceptacja i przygotowanie się banku, że ryzyko cyfrowe może się pojawić w każdym momencie i reakcja musi być wtedy błyskawiczna,
c) przestrzeganie zasad etycznych, gdyż decyzje w takich sprawach najczęściej zapadają tylko na styku człowiek – komputer, a zatem bez obecności, osądu osób trzecich, często przy złudnym przeświadczeniu uniknięcia ewentualnej kary (w rozumieniu kodeksu karnego lub w relacjach społecznych),
d) monitorowanie naruszeń i odstępstw od akceptowanych zasad etycznych i kultury ryzyka, czyli istnienie wsparcia o charakterze instytucjonalnym (np. zasady, procedury, whistleblowing),
e) odejście od dominacji funkcji kontrolnych o charakterze policyjnym na rzecz partnerskiego współdziałania różnych komórek, a zwłaszcza prawnych, ryzyka, compliance i audytu.

Nowa kultura ryzyka, w szczególności widziana przez pryzmat cyberbezpieczeństwa, wskazuje na zalety wykorzystywania zdecentralizowanych działań i modeli, w ramach których łatwiej jest osiągnąć wyżej opisany stan.

Niewątpliwie najważniejszy jest związek kultury ryzyka z jego zarządzaniem, skutecznością, zwłaszcza w instytucjach finansowych. Znajomość postaw, zachowań w organizacji pomaga zarządzać procesami, procedurami, wdrażać dobre praktyki, które są niezbędne w skutecznym zajmowaniu się ryzykiem. Dotyczy to identyfikacji czynników ryzyka, jego oceny i pomiaru, akceptacji, a skończywszy na systemie monitorowania. Zrozumiała jest też ważna rola aspektów kulturowych w systemie prowadzenia nadzoru i kontroli ryzyka przez komórki wewnętrzne banków, jak i instytucji nadzorczych. Dodatkowo świadomość roli kultury ryzyka powinna rzutować na opracowanie adekwatnych regulacji dla sektora bankowego. We współczesnych warunkach wagi nabiera znajomość nie tylko ogólnej kultury organizacyjnej instytucji finansowych, ale w szczególności stosunek i rzeczywiste postępowanie wszystkich pracowników, menedżerów wobec różnych kategorii ryzyka. Wydaje się, że niedostatecznie dostrzega się rolę kultury ryzyka w szerszym ujmowaniu

procesu zarządzania, głównie w odniesieniu do następujących obszarów, tj. strategii i modelu biznesowego, innowacji, przestrzegania regulacji (*compliance*) oraz zwracania uwagi, jak podchodzą do ryzyka klienci. W tej ostatniej kwestii lekcje mogą być bolesne, czego przykładem są doświadczenia banków związane z walutowymi kredytami mieszkaniowymi.

Rolę kultury ryzyka silniej dostrzeżono za granicą niż w Polsce. Do przytoczonych już przykładów dodać można raport The Institute Risk Management. Podkreśla on, że: „Problemy, z którymi firmy borykały się, wynikały m.in. z słabego zrozumienia ich ekspozycji na ryzyko, możliwości zmian, identyfikacji odpowiednich informacji oraz ich dostarczania najwyższemu kierownictwu, aby […] zapewniło odpowiednią kulturę ryzyka w całej firmie, a przy zwiększonej jego intensywności przygotowało się do skutecznego zarządzania kryzysowego”[10]. Podobne opinie formułują M. Power, S. Ashby, T. Palermo oraz J. Ackermann[11]. Na problematykę kultury ryzyka należy nałożyć wyzwania wynikające ze zmian technologicznych.

Przejście banków od modelu tradycyjnego do bankowości cyfrowej najlepiej odzwierciedlają proponowane modele biznesowe, które pokazują jednocześnie kierunki, jak banki mogą budować nowego typu relacje z klientami.

3. MODELE BIZNESOWE W BANKOWOŚCI CYFROWEJ

Panuje przekonanie, że cyfrowa (otwarta) bankowość będzie całkowicie odmiennym systemem obsługi klientów i funkcjonowania banków niż model tradycyjny (patrz tabela 1)[12].

Tabela 1. Typowe cechy banku XX i XXI wieku

Bank XX wieku	Bank XXI wieku
1. Materialny	1. Cyfrowy
2. Papierowy	2. Dane/digitalizacja
3. Budynki i zasoby ludzkie	3. Oprogramowanie i serwery
4. Własne rozwiązania	4. Standaryzacja/outsourcing

[10] *Risk Culture. Under the Microscope Guidance for Boards*, The Institute Risk Management, London 2012, s. 9.

[11] M. Power, S. Ashby, T. Palermo, *Risk Culture…*, *op. cit.*, s. 92; J. Ackermann, *Financial Innovation: Balancing Private and Public Interests,* [w:] M. Haliassos (red.), *Financial Innovation. Too much or Too Little*, The MIT Press, Cambridge 2013, s. 225.

[12] *The New Bank is 100% different to the Old Bank*, Skinner Blog https://thefinanser.com › Digital Bank (dostęp: 02.05.2017); O. Lingquist, C.L. Plotkin, J. Stanley, *Do you really understand how your business customers buy,* „McKinsey Quarterly”, February 2015.

Tabela 1 cd.

Bank XX wieku	Bank XXI wieku
5. Zamknięty	5. Otwarty
6. Ściśle sprzężony	6. Luźnie powiązany
7. Wolny	7. Szybki
8. Kapitałochłonny	8. Tani
9. Regulacje koncentrują się na ochronie klienta i reakcji na niepożądane działania banków	9. Regulacje to upoważnienie

Źródło: opracowanie własne na podstawie: *The New Bank is 100%…*, *op. cit*.

Nie wydaje się, aby krańcowe charakterystyki banków z tabeli 1 odpowiadały w pełni obecnym realiom rynkowym, niemniej jednak różnice są znaczące. Banki XXI wieku muszą zatem wychodzić naprzeciw zmianom, także o charakterze kulturowym. W szczególności wpisywać się w realia współczesnej, postmodernistycznej kultury konsumpcyjnej. Jej cechy opisuje tabela 2.

Tabela 2. Przesłanki i kryteria tworzenia postmodernistycznych wspólnot

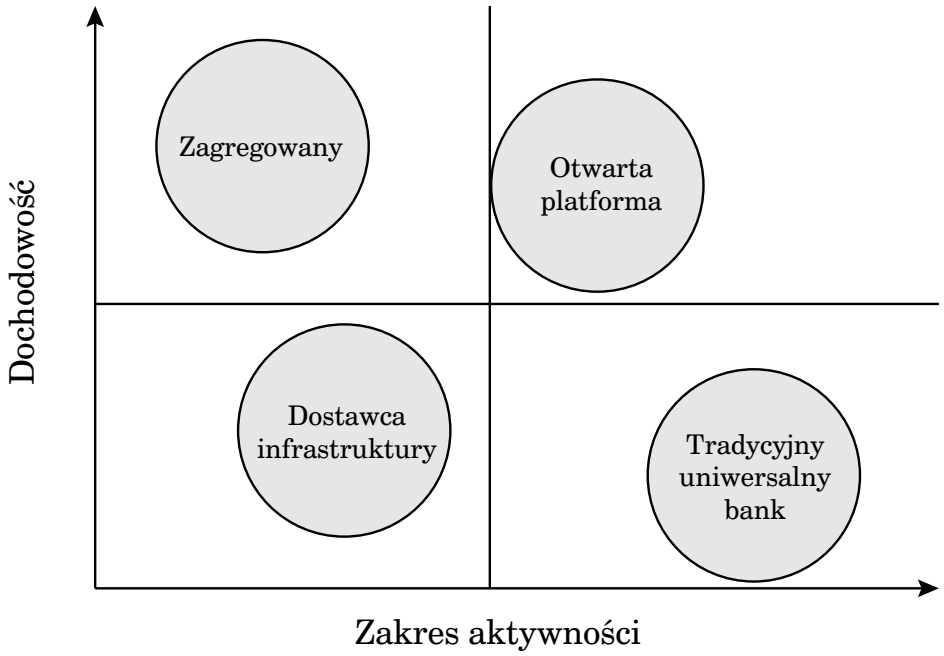
Przesłanki	Kryteria
1. Zróżnicowanie potrzeb – indywidualizm	Rodzaj zainteresowań, hobby, osobowość
2. Niepewność i poczucie zagrożenia	Rodzaj postrzeganego zagrożenia i cechy osobowości
3. Rozwój technologii internetowej	Otwartość na nowe technologie i umiejętność korzystania z nich
4. Globalizacja	Otwartość wobec procesów i produktów globalnych
5. Wzrost aktywności konsumentów na rynku	Gotowość i zdolność do prosumpcji i kształtowania rzeczywistości
6. Poszukiwanie autentyzmu i prawdy	Postawy i wrażliwość na prawdę
7. Rozwój odpowiedzialności społecznej	Poziom uspołecznienia i etyki

Źródło: K. Mazurek-Łopacińska, *Postmodernistyczna kultura konsumpcyjna w kształtowaniu popytu i stylów życia współczesnego konsumenta*, „Konsumpcja i Rozwój", nr 1/2011, s. 48.

Do głównych przesłanek tworzenia się postmodernistycznych społeczności zalicza się właśnie rozwój technologii internetowych i dążenie do bardziej nowoczesnego stylu życia. Jeśli uznamy ten kierunek za obiektywnie dziejące się zjawisko, to podmioty, które zdecydują się być bankami cyfrowymi i zamierzają zawalczyć o wysokie szanse przetrwania na rynku, muszą opracować nowe strategie konkurowania i nowe modele biznesowe. W przeciwnym razie staną się łatwymi ofiarami cyfrowej bankowości w nowej erze. Nie rozstrzygając sporu, czy ważniejsza jest strategia banku, czy biznesowa koncepcja jego działania, skoncentrujemy się na wybranych modelach. Naszym zdaniem są one podstawą do określenia mechanizmów i zasad generowania zysków, ale – co ważne, wyznaczają pozycję klienta i potencjalne ryzyka, jakie mogą mu zagrażać podczas świadczenia usług bankowych.

T. Robinson zaproponował wyróżnienie 4 typowych modeli biznesowych[13] (por. rysunek 1).

Rysunek 1. Modele biznesowe banków



Źródło: opracowanie własne na podstawie: *Four banking business models for the digital age* – Chris Skinner's Blog, https://thefinanser.com › Digital Bank, s. 1 (dostęp: 02.05.2017).

Kryterium klasyfikacji modeli bankowych na rysunku 1 uwzględnia dwa kluczowe czynniki: zakres działań biznesowych banku i przewidywaną zyskowność. **Uniwersalny model tradycyjnej bankowości** świadczy usługi samodzielnie za pomocą posiadanej infrastruktury. Ocenia się, że zakres dostarczanych usług

[13] *Four banking business models…*, *op. cit.*

dla klientów nie jest zrównoważony z infrastrukturą banku. W warunkach wysokiej konkurencji i występowania niskich marż bank staje się podmiotem o niskiej atrakcyjności dla inwestorów. **Zagregowany model**, który cechuje się wysoką rentownością i niskim poziomem intensywności zaangażowanych aktywów, wydaje się trudny do obrony. Dominuje w nim integracja pozioma, gdzie przy otwartej platformie cyfrowej specjalizacja daje możliwość uzyskiwania wysokich marż, ale naraża na silną konkurencję ze strony podmiotów niebankowych. Z kolei **model dostawcy infrastruktury** zapewnia instytucjom bankowym niskie marże, ale ich oferta oznacza wąski zakres usług. Akceptując ten model biznesowy, satysfakcjonujące wyniki osiągnie się dopiero przy wysokiej skali obrotów. Najbardziej pożądany model, o największym potencjale rozwojowym, stanowi wariant **otwartej platformy**, skupiający szeroki zakres jednostek współpracujących z bankiem i oferujących niezwykle bogatą ofertę, skuteczną, o wysokiej jakości i efektywności. Ten model generuje najwyższą zyskowność i zakres cyfrowych usług dla klienta. Opis tych modeli jest bardzo skrótowy. Pozwala jednak na naszkicowanie potencjalnych kierunków rozwoju bankowości i osadzenie w nich pozycji klienta. Jednakże i w tym przypadku przy silnym patrzeniu poprzez aspekty operacyjne.

Inny, bardziej rozwinięty w opisie model biznesowy funkcjonowania banku prezentuje A. Bollard ze współpracownikami[14]. Mimo stałego podkreślania roli klienta i stawiania go na najważniejszym miejscu, przykład ten również uzmysławia, jak trudno oderwać się od pierwszoplanowego eksponowania czynników technologiczno-organizacyjnych. Kluczowe składowe tej koncepcji ilustruje rysunek 2.

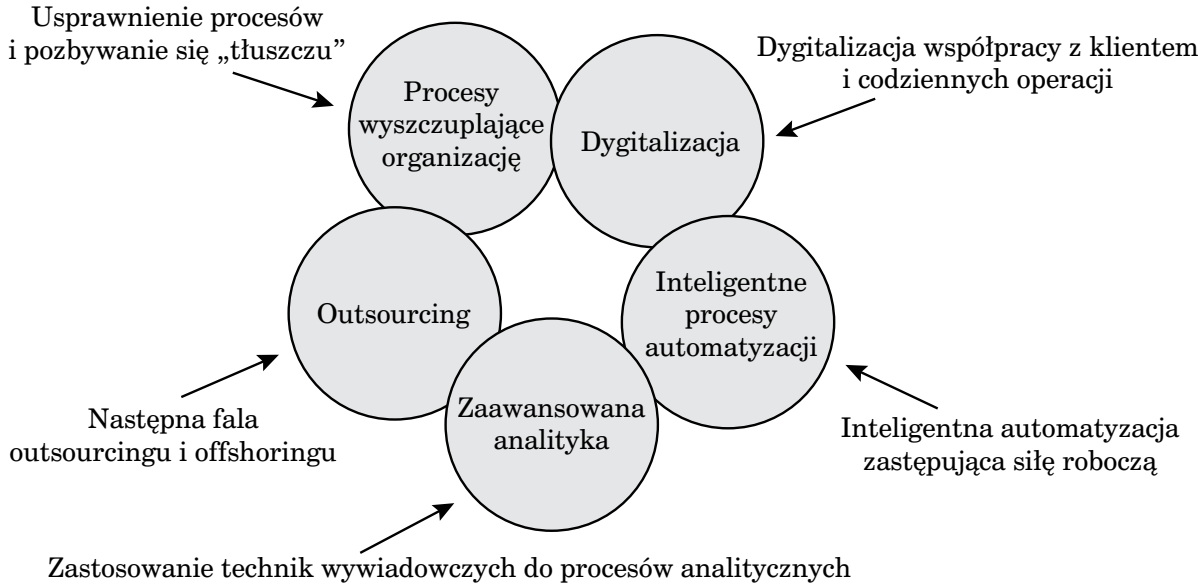
Ze schematu wynika, że sukces jego wdrożenia zależy do efektów poszczególnych etapów: codziennej cyfryzacji doświadczeń klienta, wprowadzenia inteligentnej automatyzacji czynności zastępujących te, które były dokonywane przez pracowników, ułatwienia procesów decyzyjnych przez wykorzystanie zaawansowanej analityki, outsourcingu i offshoringu oraz realizacji usprawnienia procesów i minimalizacji strat. Rekomendowany model operacyjny uwzględnia przede wszystkim aspekty menedżerskie i jakościowe, a zagadnienia zagrożeń dla klientów banków są pominięte. Znajdują się one w innych opracowaniach firmy konsultingowej McKinsey, dotyczących zarządzania ryzykiem[15].

---

[14] F. Berruti i in., *Intelligent process automation: The engine at the core of the next-generation operating model*, „Digital McKinsey", March 2017; S. Chheda, E. Duncanand S. Roggenhofer, *Putting customer experience at the heart of next-generation operating models*, „Digital McKinsey", March 2017; P. Dahlström, D. Desmet, M. Singer, *The seven decisions that matter in a digital transformation: A CEO's guide to reinvention*, „Digital McKinsey", March 2017; J. Dias i in., *How to start building your next-generation operating model*, „Digital McKinsey", March 2017; *The digital reinvention of an Asian bank*, „McKinsey Quarterly", March 2017.

[15] Lista publikacji poświęconych zarządzaniu ryzykiem zawiera 71 pozycji. Zob. P. Härle i in., *The future of bank risk management*, McKinsey Working Papers on Risk, McKinsey&Company, July 2016, s. 31–32.

Rysunek 2. Pięć aspektów zbudowania modelu operacyjnego banku następnej generacji



Źródło: opracowanie własne na podstawie: A. Bollard i in., *The next-generation operating model for the digital world*, Digital McKinsey, March 2017, s. 4.

Jak kształtować bank cyfrowy ujawnia prezes banku DGS – P. Gupta. Jego spojrzenie znajduje potwierdzenie w modelu operacyjnym pokazanym na rysunku 1[16]. Wskazuje on na ważne fazy: potrzebę na nowo przemyślenia doświadczeń klienta podczas jego „podróży usługowej”, konsekwentną determinację w procesie wdrażania pełnej cyfryzacji (bez używania dokumentów papierowych), specyficzne sposoby tworzenia i motywowania zespołów innowacyjnych, przydatność użycia nowego wskaźnika (ATE)[17] oraz wagę kultury cyfrowej. Czynniki kulturowe, zdaniem P. Gupta, odpowiadają na fundamentalne pytanie: „czy jesteś w stanie stworzyć firmę, która ma zdolność adaptacyjną, energię i zręczność, a zdecydowana większość pracowników jest skłonna do działania i myślenia jak przedsiębiorcy?”[18]

---

16 *The digital reinvention of an Asian bank*, „McKinsey Quarterly”, March 2017.

17 Wskaźnik ATE należy czytać w następujący sposób: A (*acquisition*) oznacza pozyskanie klientów za pośrednictwem narzędzi cyfrowych w Internecie. T (*transaction*) odnosi się do transakcji, polegających na operacyjnym, elektronicznym przetwarzaniu danych bez udziału czynnika ludzkiego ze strony instytucji finansowej, czyli bez ręcznego ich wprowadzania. E (*engagement*) jest najtrudniejsze do określenia, a dotyczy stopnia zaangażowania, zaabsorbowania klienta przez wymogi operacyjne. Mierzy się tę wielkość poprzez różnicę w ilości produktów (transakcji) kupowanych (przeprowadzaniach) przez klientów w sytuacji, gdy są one w pełni zdygitalizowane w stosunku do tych nie objętych cyfryzacją.

18 *The digital reinvention…*, *op. cit.*

W świetle powyższych spostrzeżeń na podkreślenie zasługuje stanowisko Federal Trade Commission. Zawraca ona uwagę na czynniki ryzyka, które nie są czytelnie identyfikowane w analizowanych modelach biznesowych banków, ale mają istotny wpływ na zagrożenia dla klientów[19]:

a) złośliwe oprogramowanie,
b) hakerzy,
c) nieautoryzowany dostęp do danych (dostęp cyfrowy i fizyczny),
d) rozkonfigurowanie zasobów informacyjnych,
e) nieprawidłowe przechowywanie informacji wrażliwych,
f) utracone lub nieprawidłowe nośniki kopii zapasowych,
g) utrata informacji poprzez likwidację aktywów informatycznych,
h) sprzęt komputerowy osobisty,
i) nieprawidłowa transmisja danych.

Reasumując, można stwierdzić, że omawiane cyfrowe modele biznesowe wymuszają w banku inne wartości, postawy i zachowania wszystkich pracowników w stosunku do: akceptacji „apetytu" na ryzyko, jego pomiaru, odpowiedzialności, podejmowania działań ograniczających zagrożenia, systemu komunikacji i przyjętego modelu kultury ryzyka w ciągłych relacjach pracowników banku z klientami, niż to ma miejsce w większości funkcjonujących banków w Polsce. Aktualnie system zarządzania ryzykiem w bankach jest wysoce przeregulowany, nadmiernie zbiurokratyzowany, koncentrujący się w departamentach ryzyka i audytu, słabo reagujący na nowe rodzaje ryzyka i w rezultacie wysoce pracochłonny oraz kosztowny.

4. AKTUALNE I POTENCJALNE RODZAJE RYZYKA KLIENTA CYFROWEGO

Panuje niemal powszechne przekonanie, że ryzyko cyfrowe powinno być traktowane priorytetowo przez zarządy banków, regulatorów i nadzorców[20]. W praktyce zależy to od przyjętej strategii banku, jego modelu biznesowego, stopnia zaawansowania w budowie instytucji cyfrowej i intensywności konkurowania na rynku usług cyfrowych. Dominująca część publikacji rozpatruje te rodzaje ryzyka z perspektywy banków, a zagrożenia dla klientów stanowią tylko element uzupełniający. Tym bardziej tematyka ta wymaga uwagi, a o jej skali i znaczeniu świadczy mnogość zagrożeń związanych z funkcjonowaniem w świecie cyfrowym. Do kluczowych zalicza się:

1) ryzyko destrukcji cyfrowej banków,
2) ryzyko przestępstw i oszustw cyfrowych,

---

[19] *Data Center General Support System (Data Center GSS)*, Federal Trade Commission. Privacy Impact Assessment, Updated December 2016, s. 12–13.

[20] *Banking risk in the digital age*, Quarterly Outlook, Parker Fitzgerald, Transforming Financial Services, May 2016, s. 1.

3) ryzyko braku kultury cyfrowej,
4) ryzyko regulacyjne,
5) ryzyko wynikające z wdrożenia nowych technologii,
6) ryzyko biznesowego modelu cyfrowego.

Ad 1) Ryzyko destrukcji cyfrowej banków

Innowacje technologiczne i finansowe, jakie towarzyszą implementacji nowej koncepcji kształtowania usług bankowych na otwartej platformie cyfrowej, cechuje jednocześnie transformacja i częściowo destrukcja niektórych procesów, zwłaszcza tych, które funkcjonują w tradycyjnym modelu, bądź zbyt powolnie dostosowują się do nowych wyzwań. Jednym z takich widocznych działań jest proces ograniczania wielkości i liczby klasycznych oddziałów bankowych. Jednocześnie redukuje się też ich funkcje, wyposażenie oraz strukturę zawodową pracowników. W niektórych bankach proces ten przebiega dość dynamicznie. Na drugim biegunie obserwujemy zupełnie inne podejście do klientów ze strony fin-techów. Wymusza to na dotychczasowych instytucjach finansowych przyjmowanie innowacyjnych strategii i modeli biznesowych. Prowadzi też do spadku ogólnego zatrudnienia w sektorze bankowym[21].

Wykorzystanie rozwiązań integracyjnych i funkcjonowanie w układzie sieciowym, gdzie liczba wzajemnych połączeń podmiotów operujących na rynku cyfrowym może być niebotycznie duża, sprawia, że klient w bardzo krótkim czasie (liczonym w sekundach) może zarówno odnieść korzyści, jak i narazić się na dotkliwe straty. Dlatego też narasta problem posiadania odpowiedniej wiedzy przez klientów i systematycznego jej uzupełniania, aby nie stać się ofiarą wykorzystania zawansowanych technologii. Instytucje świadczące usługi bankowe działające na platformie cyfrowej oferują, z jednej strony prostotę, wygodę, szybkość, profesjonalne doradztwo, dostępność i łatwość zawarcia transakcji, a z drugiej strony kreują też poważne ryzyka. Co więcej, w procesie transformacji i destrukcji systemu bankowego klienci narażeni są na to, że część banków i instytucji płatniczych czy finansowych może nie być zdolna do sprostania wymogom konkurencyjnym i po prostu zbankrutować. Potencjalna skala tego zjawiska jest trudna do przewidzenia, ale dodatkowo istnieje zagrożenie pojawienia się efektu zarażenia. Tego typu zjawiska mogą spowodować, obok wielu negatywnych skutków ekonomicznych, społecznych czy nawet politycznych, również straty klientów części lub całości swoich oszczędności. Powszechny system gwarantowania depozytów w bankach

[21] W raporcie Parker Fitzgerald podaje się, że inwestycje w Fin-Techy w okresie 2010–2015 wzrosły z poziomu 2 mld $ do 19 mld $. Ponadto szacuje się, że tradycyjne banki stracą do 30% przychodów do 2026 roku, a poziom zatrudnienia pracowników na pełnym etacie obniży się o ok. 25% w stosunku do okresu przedkryzysowego. Co ważne, dynamika tych procesów utrzyma się na wysokim poziomie po 2026 r. *Ibidem*, s. 8.

zapewnia ochronę do równowartości 100 tys. euro, ale już nie obejmuje środków jednostek samorządu terytorialnego. Także dla większych firm poziom gwarancji jest symboliczny.

Ad 2) Ryzyko przestępstw i oszustw cyfrowych

Ryzyko cyfrowe wiąże się przede wszystkim z wykorzystaniem internetu, prowadzeniem handlu internetowego, systemami i sieciami elektronicznymi, z przechowywaniem osobowych baz danych. Wobec wzrostu ich znaczenia, ryzyko cyfrowe zalicza się do kluczowych rodzajów zagrożeń, z jakimi przychodzi się zmierzyć bankom. Dlatego też starają się zarządzać tą sferą, aby ponosić jak najmniejsze straty pieniężne, ale także reputacyjne. W 2015 r. ataki hakerskie dotknęły 19% polskich instytucji finansowych, zaś w 2016 r. już 37%[22]. Raport FireEye podkreśla trzy zjawiska[23]. Po pierwsze, że ryzyko przestępstw i oszustw cyfrowych dramatycznie intensyfikuje się[24]. Zagraża nie tylko utratą ważnych danych finansowych i osobowych, ale tworzy niebezpieczeństwa dla niezawodnego działania zakładów produkcyjnych, elektrowni, infrastruktury lotniczej, transportowej, a nawet elektrowni atomowych wraz z rozwojem tzw. internetu rzeczy. Może też mieć istotny wpływ na wyniki wyborów politycznych (wybory prezydenckie w USA, referendum w sprawie Brexitu). Po drugie, zauważa dużą rolę regulacyjnej aktywności UE w zakresie ochrony danych osobowych. Po trzecie, formułuje apel do zarządów instytucji i firm, aby nie czekały bezczynnie na skuteczne regulacje lub działania organów państwowych, ale włączyły się aktywnie w redukowaniu tego rodzaju ryzyka.

W ramach ryzyka cyfrowego wyróżnić można podstawowe jego obszary. T. Olsen wyodrębnia następujące[25]: ataki hakerskie, naruszenie bezpieczeństwa danych, szantaże cyfrowe, transmisja wirusów, sabotaż pracowników, przestoje w funkcjonowaniu sieci, nieodpowiedzialne działania mediów, błędy ludzkie. Okazuje się, że nad Europą kumuluje się największe zagrożenia cyfrowe, a sektor finansowy poddawany jest najsilniejszym atakom już wysoce profesjonalnych grup dokonujących przestępstw i oszustw cyfrowych. W 2016 r. M. Malinowski podaje, że wśród ankietowanych przedsiębiorstw do największych cyberzagrożeń zalicza się złośliwe oprogramowanie i phishing[26].

---

22 J. Patyńska, *Unia zrywa zmowę milczenia*, „Bank" 2017, nr 3, s. 66.

23 *2017 Cyber threats: A perfect storm about to hits Europe?*, Fireeye Marsh & McLennan Cyber Risk Report, Special Report, s. 3.

24 Potwierdza to wydarzenie jakie miało miejsce w 2016 r., kiedy to nastąpił największy atak hakerski na polskie banki. W wyniku tego komputery klientów 230 banków spółdzielczych i 17 komercyjnych zostały zainfekowane wirusem. Bardziej zuchwały był atak na infrastrukturę KNF. Zob. M. Malinowski, *Na celowniku cyberszpiegów*, „Bank" 2017, nr 3, s. 117.

25 T. Olsen, *Insurance Cyber Risk*, Willis, 18.06.2013, s. 7. https://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf (dostęp: 08.04.2017).

26 M. Malinowski, *Na celowniku…*, *op. cit.*, s. 117.

Ad 3) Ryzyko braku kultury cyfrowej

Zagrożenia cyberprzestępczości związane są także z cechami kultury cyfrowej klientów, pracowników banków, instytucji regulacyjnych i nadzorczych. Niski poziom tego rodzaju kultury, wynikający ze słabego poziomu wykształcenia, braku elementarnej wiedzy finansowej i informatycznej, niechęci do uczenia się, z jednoczesną dążnością do jak najszybszego wzbogacenia się, może powodować poważne straty finansowe klientów. Taki scenariusz jest wysoce prawdopodobny, zwłaszcza gdy dodamy nierzadkie przekonanie (świadomie lub podświadomie), że w razie nieszczęścia państwo weźmie na siebie ciężar złagodzenia skutków niefrasobliwych decyzji (patrz efekt „frankowiczów").

Od strony kulturowej również postawy i zachowania pracowników oraz kierownictw banków, wykorzystujące świadomie słabości klientów, brak umiejętności wsłuchiwania się w ich potrzeby, są czynnikami ryzyka. Dlatego H. Fanderl, K. Neher i A. Pulido propagują potrzebę systematycznego mierzenia głosu klienta i jego integracji z kulturą ciągłego sprzężenia zwrotnego między bankiem a odbiorcą usług cyfrowych[27]. Zalecają stosowanie specjalnej metodyki pomiaru głosu klienta, którą określają jako „piramidę pomiaru doświadczeń klienta" (*Customer-experience-measurement pyramid*).

Ad 4) Ryzyko regulacyjne

Generalnie opinia o współczesnych regulacjach rynku innowacji finansowych, technologicznych czy ochronie praw osobowych jest taka, że nie nadążają one za zmianami, nie stymulują pozytywnie tych procesów i stanowią istotną przeszkodę rozwojową. Wydaje się, że wielce obiecujące dla ochrony praw osób fizycznych jest Rozporządzenie Parlamentu Europejskiego i Rady UE z 27 kwietnia 2016 r. *General Data Protection Regulation* (GDPR)[28]. Mówi ono, że instytucje finansowe mają 2-letni okres na wdrożenie przepisów, tj. do 25 maja 2018 r. Mimo że regulacja ta zachowuje zasady i terminologie przyjęte w dyrektywie z 1995 r., wprowadza jednak wiele nowych przepisów dotyczących: ostrzejszych warunków zgody na przetwarzanie danych, prawo do bycia zapomnianym, konieczność ujawniania wycieków informacji w ciągu 72 godzin, przymus podawania do publicznej wiadomości naruszeń bezpieczeństwa, surowsze kary za nieprzestrzeganie wymogów do wysokości 4% rocznego obrotu (lub 2 mln Euro, w zależności, która z tych wielkości jest wyższa)[29].

---

[27] H. Fanderl, K. Neher i A. Pulido, *Are you really listening to what your customers are saying*, McKinsey& Company, March 2016, s. 1.

[28] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation) (dostęp: 08.04.2017).

[29] *Ibidem.*

Konieczność opracowania i wdrożenia nowej regulacji w stosunku do dyrektywy z 1995 r. wynikła z następujących przesłanek[30]:

- ❖ eliminowania niespójności w przepisach krajowych;
- ❖ podwyższenia wymagań w celu zapewnienia lepszej ochrony prywatności osobom fizycznym;
- ❖ uaktualnienia prawa w celu lepszego rozwiązywania współczesnych wyzwań związanych z prywatnością, takich jak te, które stwarzają Internet, społeczne media, aplikacje mobilne, cloud computing, Big Data i marketing behawioralny, które były w fazie początkowego rozwoju, gdy prowadzono pracę nad dyrektywą o ochronie danych;
- ❖ ograniczenia kosztownych obciążeń administracyjnych dla firm podlegającym kontroli wielu organów ochrony danych.

Nie kwestionując zasadności tego rozporządzenia powstaje wątpliwość, czy omawiane rozwiązania regulacyjne nie spowodują załamania równowagi między dotychczasową pozycją i funkcjami banku a interesami jego klientów. Najgorsza byłaby sytuacja, gdyby percepcja banków uznała tę regulację za nadmierną, nie liczącą się z kosztami, jakie potencjalnie mogą one ponosić dla ochrony swoich klientów, a w konsekwencji podjęta zostałaby walka z nią lub jej omijanie. Niestety, dotychczas nie przeprowadzono badań w obszarze oceny ryzyka regulacyjnego w sferze związanej z ochroną klienta cyfrowego.

Ad 5) Ryzyko wynikające z wdrożenia nowych technologii

Technologie rozwijają się w tempie wykładniczym, natomiast regulacje i ich wdrażanie zdecydowanie wolniej. Asychroniczność tych procesów może powodować liczne zagrożenia związane z wyborem (blokadą) technologii, tym bardziej że banki nie ograniczają się do wykorzystania tylko jednego ich rodzaju. Ponadto z dnia na dzień mogą być zaskakiwane licznymi innowacjami. W literaturze fachowej rekomenduje się od 5 do 10 kluczowych rozwiązań teleinformatycznych dla zbudowania banku cyfrowego i wobec tego pozostaje do rozstrzygnięć zarządów i właścicieli banków, w jakiej kolejności i w jakiej skali te technologie implementować. Liczne i poważne zagrożenia z nimi związane mogą wynikać z tego, że niektóre rozwiązania wymagają posiadania wysoce utalentowanych specjalistów i przeprowadzenia dużego zakresu szkoleń niemal wszystkich grup pracowników w jednym czasie. Co więcej, pewne innowacje, np. sztuczna inteligencja, automatyzacja procesów obsługi klientów, mogą wpływać na poważną redukcję personelu, co wymaga opracowania elastycznej strategii rozwoju kadr i skutecznego systemu motywacyjnego, sprzyjającego odejściu od tradycyjnych, silosowych rozwiązań na rzecz stymulowania wyższego poziomu współpracy wewnątrz banku i z firmami zewnętrznymi.

---

[30] W.S. Blackmer, *GDPR: Getting Ready for the New EU General Data Protection Regulation*, May 5, 2016, s. 1.

Wydaje się, że największym zagrożeniem w obszarze technologicznym jest uzyskanie wysokiego poziomu ich wykorzystania, który by generował zadowalający poziom rentowności banku, co jest uwarunkowane nie tylko posiadaniem talentów, ale wysokim ich zaangażowaniem i wysoką umiejętnością szybkiego uczenia się oraz zdolnością wykorzystania pojawiających się okazji.

Ad 6) Ryzyko biznesowego modelu cyfrowego

Transformacja banku tradycyjnego w kierunku cyfrowego wymaga zmiany i opracowania całkowicie nowego modelu biznesowego. Niektórzy wyobrażają sobie bank, który świadczy usługi bankowe, ale jego dominującą działalnością staje się produkcja specjalistycznego oprogramowania. Zrozumiałe jest, że te instytucje, które decydują się na opracowanie cyfrowej strategii i modelu biznesowego, czeka wiele pułapek, nietrafionych decyzji i zagrożeń. Czynnikami ryzyka może być brak takowego modelu lub przyjęcie nieadekwatnego podejścia, wynikającego z mylnej oceny posiadanych zasobów, optymistycznej wizji, co do możliwości osiągania celów finansowych, opieranie się na nietrafionych założeniach, zastosowanie nieefektywnego systemu motywacji, przyjęcie niewłaściwej komunikacji z klientami lub pracownikami itp. Te rodzaje ryzyka są wysoce prawdopodobne, gdyż w bankach dominuje kultura biurokratyczna (np. zaproponowana przez R. Harrisona kultura roli: stabilność, uporządkowanie, racjonalność, legalność, odpowiedzialność, funkcjonalizm, kompetencje, procedury, hierarchiczność, bezpieczeństwo[31] lub przez K.S. Camerona i R.E. Quinna kultura hierarchii: sprawność, terminowość, kontrola, nastawienie na procedury, koordynacja, planowanie), a nie kultura adhokracji (przedsiębiorczość, kreatywność, innowacyjność, wzrost, podejmowanie ryzyka, nastawienie na przyszłość)[32]. Ta ostatnia charakterystyczna jest dla podmiotów zwinnych, elastycznych z jakimi mamy do czynienia na rynku fin-techów. Dotyczy to różnych sfer, np. rozwiązań menedżerskich, akceptacji prawa do pomyłki etc. Niepewne jest też otoczenie i uwarunkowania makroekonomiczne czy globalne. Wystąpienie ryzyka modelu biznesowego może wynikać z niedocenianego faktu, że trzeba dokonać w krótkim czasie kompleksowych zmian we wszystkich kluczowych elementach zarządzania bankiem, w warunkach narastającej i nieznanej konkurencji oraz zdecydowanym odejściu od zdobytego know-how i doświadczenia w realiach tradycyjnej bankowości.

---

[31] Zob. R. Harrison, *Understanding your Organization's Character*, Harvard Business Review, Boston 1972.

[32] Zob. K.S. Cameron, R.E. Quinn, *Kultura organizacyjna – diagnoza i zmiana. Model wartości konkurujących*, Oficyna Ekonomiczna, Kraków 2003.

6. PODSUMOWANIE

Rozpatrując zagrożenia dotyczące cyfrowego świadczenia usług finansowych, koncentrujemy swoją uwagę na aspektach technologicznych i cyberprzestępczości. Można jednak, i należy, spojrzeć na to zagadnienie także od strony kluczowej postaci jaką jest człowiek, występujący jako klient, pracownik lub menedżer banku, regulator, nadzorca, a także przestępca. Dlatego też jego zachowania, nawyki, poczucie bezpieczeństwa, otwartość na nowości, umiejętności, wiedza itd., czyli aspekty psychologiczno-kulturowe, należą do ważnych determinant rozwoju bankowości elektronicznej. Dlatego też otaczająca i tkwiąca w nas kultura determinuje nie tylko ryzyko związane z cyfrową stroną modeli biznesowych, ale przenika do wszystkich aspektów działania banków w zupełnie nowych uwarunkowaniach zewnętrznych i wewnętrznych. Na tle przedstawianego wywodu nasuwa się wniosek, że rozpatrując pozycję klienta i związane z nim ryzyko w dobie bankowości cyfrowej nie należy zwracać uwagi tylko na aspekty technologiczne, ale także kulturowe. Zwłaszcza kultura ryzyka należy do kluczowych determinant sukcesów instytucji finansowych. Potwierdza tę konstatację waga jaką do tego zagadnienia zaczęły przykładać organy nadzorcze (niestety, banki już mniej) i doświadczenia wskazujące, że nawet najlepsze regulacje pozostaną martwe bez odpowiednich postaw, zachowań, przestrzegania wartości. W Polsce przykładami (choć nie związanymi z cyberzagrożeniami) są upadłości SK Banku w Wołominie i Banku Spółdzielczego w Nadarzynie. Mimo istnienia i wprowadzenia nowych, formalnych, daleko idących wymogów ostrożnościowych to człowiek zawiódł, a szczególnie jego postawa wobec ryzyka i nieuczciwość. Są to przypadki skrajne, wręcz kryminalne. Patrząc jednak bardziej ogólnie mamy do czynienia ze współczesnym paradoksem. Istota działalności bankowej sprowadza się do umiejętnego zarządzania ryzykiem i z tego powodu podlega licznym regulacjom oraz kontroli, ale w praktyce czynniki kulturowe mogą mieć niebagatelne znaczenie, a niestety są bardzo często niedoceniane przez banki. Tym bardziej jest to ważne, gdyż do głównych zagrożeń doszła cała paleta związana z rozwojem bankowości cyfrowej.

Streszczenie

Wysoka dynamika zmian w technologiach i modelach biznesowych współczesnych banków skłania do zbadania, czy pozycja klienta cyfrowego nie stanie się najsłabszym czy najbardziej zaniedbanym obszarem w ich działalności, a także w pracach regulatorów i nadzorców rynku usług bankowych. Przedmiotem rozważań jest identyfikacja zagrożeń, jakie mogą spotkać klienta cyfrowego. Treść dotyczy trzech obszarów, z reguły badanych w sposób autonomiczny: ochrony klienta bankowego, kultury ryzyka i odchodzenia od tradycyjnych modeli bankowości na

rzecz cyfrowych. Celem artykułu jest porównanie ryzyka klienta w dotychczasowym modelu bankowości z zagrożeniami związanymi z transformacją sposobów działania banków, głównie ze względów technologicznych i kulturowych. Pojawianie się diametralnych różnic w istocie i w podejściu do ryzyka klienta cyfrowego w stosunku do obecnie dominujących mechanizmów i koncepcji zarządzania ryzykiem bankowym oznacza zmiany dla wszystkich uczestników rynku. Uwarunkowania technologiczne wymuszają nową klasyfikację ryzyka klienta, która powinna uwzględniać również czynniki kulturowe. Ich znaczenie wzrasta i zakwalifikować je można do głównych determinant funkcjonowania oraz rozwoju banków. Kategoryzacja ryzyka jest w systemie zarządzania ryzykiem kluczowym etapem, który decyduje o kolejnych np. jego pomiarze, działaniach na rzecz ograniczania, monitorowania czy raportowania. Omawiana problematyka przedstawiana jest na tle polskiego rynku usług bankowych, który w stosunku do innych krajów UE cechuje się nie tylko stabilnością, bezpieczeństwem, ale również wysoką innowacyjnością. Współczesny paradoks ujawnia się w tym, że istota działalności bankowej sprowadza się do umiejętnego zarządzania ryzykiem i z tego powodu podlega licznym regulacjom i kontroli, ale w praktyce banki w minimalnym zakresie uwzględniają czynniki kulturowe.

Słowa kluczowe: bankowość cyfrowa, kultura, innowacje

Abstract

The high dynamics of changes in technologies and business models of modern banking are driving to the question whether the position of a digital customer will not become the weakest or the most neglected area in bank operations, and one of key problems for regulators and supervisors. The subject of consideration is dedicated to identification of threats for a digital customer. The article concerns three areas, usually analyzed autonomously: protection of the client, risk culture and transformation from traditional banking model to a digital one. The aim of the analysis is to compare the client's risk in the current banking model with the risks associated with the transformation of bank operations, mainly due to technological and cultural reasons. The appearance of diametric differences in the essence and the approach to digital client risk in relation to the prevailing mechanisms and concepts of banking risk management will have consequences for all market participants. Technological circumstances on force a new classification of the client's risk, which should take into account cultural factors. The importance of cultural aspects increases and they belong to the main determinants of functioning and development of banks. Risk categorization is a key step in a risk management system, which determines, for example, its measurement, mitigation, monitoring and reporting. The discussed issues are presented in the context of the Polish

banking market. It is not only characterized by stability, security but also high innovativeness. The contemporary paradox is revealed in the fact that the essence of banking activity is based on the proper risk management (reason for numerous regulations and controls), but in practice the banks take into account important, cultural factors to a minimal extent.

Key words: digital banking, culture, innovations

Bibliografia

Banking Conduct and Culture: A Call for Sustained and Comprehensive Reform. Monograph, Group of Thirty, Washington, D.C., July 2015.

Banking risk in the digital age, Quarterly Outlook, Parker Fitzgerald, Transforming Financial Services, May 2016.

Berruti F., Nixon G., Taglioni G., Whitemanet R., *Intelligent process automation: The engine at the core of the next-generation operating model*, Digital McKinsey, March 2017.

Blackmer W.S., *GDPR: Getting Ready for the New EU General Data Protection Regulation,* May 5, 2016.

Bollard A., Larrea E., Singla A., Sood R., *The next-generation operating model for the digital world*, „Digital McKinsey", March 2017.

Cameron K.S., Quinn R.E., *Kultura organizacyjna – diagnoza i zmiana. Model wartości konkurujących*, Oficyna Ekonomiczna, Kraków 2003.

Chheda S., Duncanand E., Roggenhofer S., *Putting customer experience at the heart of next-generation operating models*, „Digital McKinsey", March 2017.

2017 Cyber threats: A perfect storm about to hits Europe? Fireeye, Marsh & MCcLennan Cyber Risk Report. Special Report. Dahlström P., Desmet D., Singer M., *The seven decisions that matter in a digital transformation: A CEO's guide to reinvention*, „Digital McKinsey", March 2017.

Data Center General Support System (Data Center GSS), Federal Trade Commission. Privacy Impact Assessment, Updated December 2016.

Dias J., Hamilton D., Paquette Ch., Sood R., *How to start building your next-generation operating model*, „Digital McKinsey", March 2017.

Dudley W., *Enhancing Financial Stability by Improving Culture in the Financial Services Industry.* Remarks at The Workshop on Reforming Culture and Behavior in the Financial Services Industry, Federal Reserve Bank of New York, October 20, 2014.

Fanderl H., Neher K., Pulido A., *Are you really listening to what your customers are saying*, McKinsey & Company, March 2016.

Four banking business models for the digital age, Chris Skinner's Blog, https://thefinanser.com › Digital Bank (dostęp: 02.05.2017).

Guidance on Supervisory Interaction with Financial Institutions on Risk Culture. A Framework for Assessing Risk Culture, Financial Stability Board, 7 April 2014.

Härle P., i in., *The future of bank risk management,* McKinsey Working Papers on Risk. McKinsey & Company, July 2016.

Harrison R., *Understanding your Organization's Character*, Harvard Business Review, Boston 1972.

High level principles for risk management, Committee of European Banking Supervisors, London, 2014, https://www.eba.europa.eu/documents/10180/16094/HighLevelprinciplesonriskmanagement.pdf (dostęp: 15.03.2017).

Lingquist O., Plotkin C.L., Stanley J., *Do you really understand how your business customers buy,* „McKinsey Quarterly", February 2015.

Maciąg P., *Wirtualna a doskonała konkurencja*, „E-mentor" 2016, nr 5(67).

Malinowski M., *Na celowniku cyberszpiegów*, „Bank" 2017, nr 3.

Managing change and risk in the age of digital transformation. The digital journey of financial institutions in ASEAN, E&Y Report, Singapore 2016.

Mazurek-Łopacińska K., *Postmodernistyczna kultura konsumpcyjna w kształtowaniu popytu i stylów życia współczesnego konsumenta*, „Konsumpcja i Rozwój", nr 1/2011.

Monkiewicz J., *W poszukiwaniu nowego paradygmatu ochrony konsumentów na rynkach finansowych*. Referat na konferencję *Jak chronić konsumenta na rynku finansowym? Modele i doświadczenia międzynarodowe,* Rzecznik Finansowy, Warszawa 11.10.2017.

Ochs S., *Inside the Banker's Brain: Mental Models in the Financial Services Industry and Implications for Consumers*, *Practitioners and Regulators*, Monograph, Initiative on Financial Security, The Aspen Institute, 2014.

Olsen T., *Insurance Cyber Risk*, Willis, 18.06.2013, https://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf (dostęp: 08.04.2017).

Patyńska J., *Unia zrywa zmowę milczenia*, „Bank" 2017, nr 3.

Power M., Ashby S., Palermo T., *Risk Culture in Financial Organizations: Final Report*, Financial Services Knowledge Transfer Network, London 2013, www.lse.ac.uk/researchAndExpertise/units/CARR/pdf/Final (dostęp: 14.04.2017).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (dostęp: 08.04.2017).

The digital reinvention of an Asian bank, „McKinsey Quarterly", March 2017.

The New Bank is 100% different to the Old Bank, Skinner Blog https://thefinanser.com › Digital Bank (dostęp: 02.05.2017).