PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1081 — 2005
Nowoczesne technologie informacyjne w zarządzaniu

Grzegorz Kotliński

WYBRANE ASPEKTY ZAPEWNIENIA BEZPIECZEŃSTWA INFORMACYJNEGO BANKU

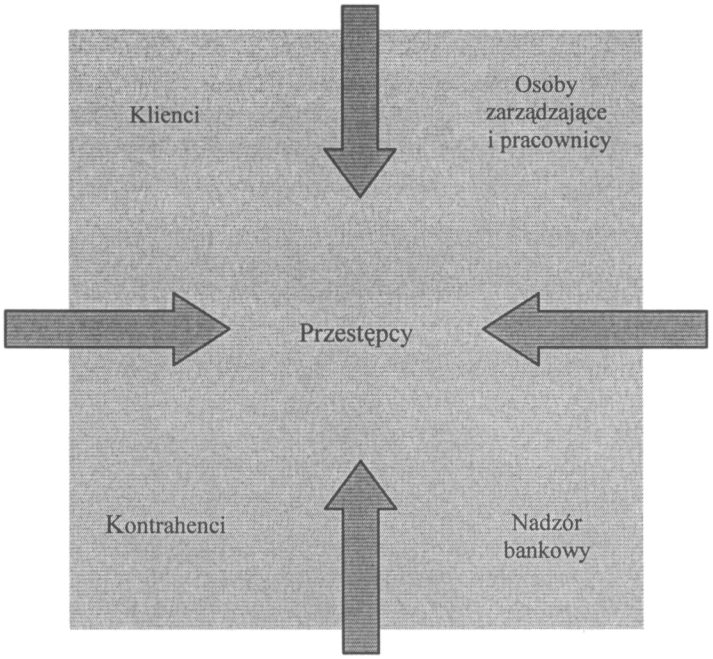
1. Wprowadzenie

Zapewnienie bezpieczeństwa nie jest dla zarządzających bankiem problemem nowym. Ostatnie 15 lat przyniosło w tym względzie radykalne przeobrażenia [Janc 2004, s. 8]. Najłatwiej zauważyć zmianę przedmiotu troski menedżerów. Poprzednio bezpieczeństwo starano się zapewnić (w kolejności) klientom, pracownikom i pieniądzom zgromadzonym w kasach banków. Era informacyjna wymusiła położenie szczególnego nacisku na zapewnienie bezpieczeństwa informacjom krążącym w banku. Sprostanie poszerzonym wymaganiom związane jest z nakładami, których wartość determinuje wyniki finansowe banków. Trudno się zatem dziwić, że tak wydatnie wzrosło zainteresowanie zarządzających polityką zapewnienia bezpieczeństwa informacyjnego. Dąży się do integracji przedsiębranych działań oraz do nadania im cechy kompleksowości. Tworzona w bankach polityka zapewnienia bezpieczeństwa obejmuje szeroki zakres istniejących metod i dostępnych środków.

2. Bezpieczeństwo banku i jego postrzeganie przez grupy interesariuszy banku

Bezpieczeństwo banku to nieuchwytny iabstrakcyjny cel dążeń; abstrakcyjny tym bardziej, że jest to kategoria pojmowana relatywnie. Łatwiej określić, który z porównywanych banków jest bardziej bezpieczny niż stwierdzić, że pojedynczy bank zapewnia bezpieczeństwo. Co ważne, tak jak modelowo przedstawiono to na rys. 1, bezpieczeństwo jest wartością, którą każda z grup interesariuszy banku postrzega inaczej, a jego rzeczywisty poziom zależy od umiejętności i wiedzy (lub niewiedzy i braku umiejętności) przestępców, którzy co prawda w sposób negatywny, lecz

ostateczny określają poziom bezpieczeństwa banku. Pozostałe grupy interesariuszy banku mają na ten temat wiedzę subiektywną, z reguły daleką od prawdy.

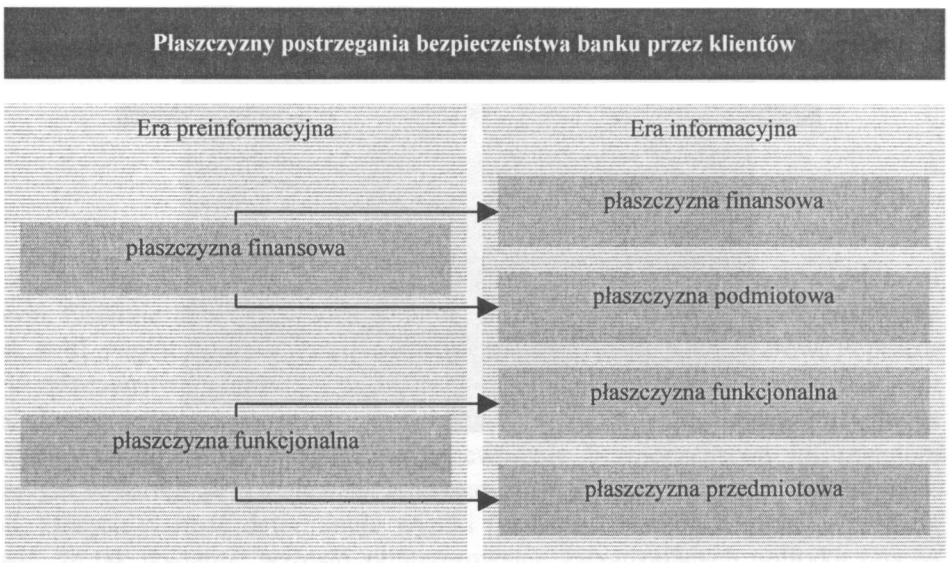


Rys. 1. Postrzeganie bezpieczeństwa informacyjnego banku
Źródło: opracowanie własne.

Bezpieczeństwo banku, w uwarunkowaniach ery informacyjnej, należy postrzegać z uwzględnieniem czterech płaszczyzn – finansowej i podmiotowej, funkcjonalnej i przedmiotowej. Wszystkie cztery wspólnie podsuwają klientom kryteria, których spełnienie pozwala postrzegać działalność danego banku jako mniej lub bardziej bezpieczną. Modelowy schemat przemian w tym zakresie przedstawiono na rys. 2.

Rozpatrując bezpieczeństwo banku od strony podmiotowej, należy zauważyć, że bank jest tym bardziej bezpieczny, im za bardziej bezpieczny uważają go jego klienci. Odczucia klientów silnie uzależnione są od ich poglądów na temat bezpieczeństwa zdeponowanych środków i pewności wykonania transakcji zlecanych bankowi. Wielkie znaczenie mają tradycje współpracy (z przeszłości) oraz obiegowe opinie powtarzane w środowiskach, w których obracają się konkretni klienci banku. Pozostaje tu nawet margines na odpowiednie działania marketingowe, które mogą, w krótkich okresach, mieć wpływ na poglądy partnerów banku. Bezpieczeństwo zdeponowanych w banku środków pieniężnych w erze preinformacyjnej uzależnione było li tylko od sytuacji finansowej banku, a ściślej od poziomu jego

płynności i sytuacji kapitałowej. Rewolucja informacyjna spowodowała, że ważne jest nie tylko to, czy bank spełnia finansowe wymagania bezpieczeństwa, ale także i to, czy potrafi docierać z takimi informacjami do klientów i kontrahentów banku. Stanowi ona wielkie zagrożenie. Może się zdarzyć, że bank spełniający wszelkie konieczne wymagania finansowe zapewniające mu w tym względzie bezpieczeństwo, stanie się celem ataku informacyjnego bliżej nieokreślonej dziś grupy przestępców, rozpowszechniających dane nieprawdziwe, tylko po to by wzbudzić wątpliwości wśród jego klientów i zachęcić ich do wycofania wkładów.



Rys. 2. Porównanie płaszczyzn postrzegania przez klientów bezpieczeństwa banku w erze preinformacyjnej i informacyjnej

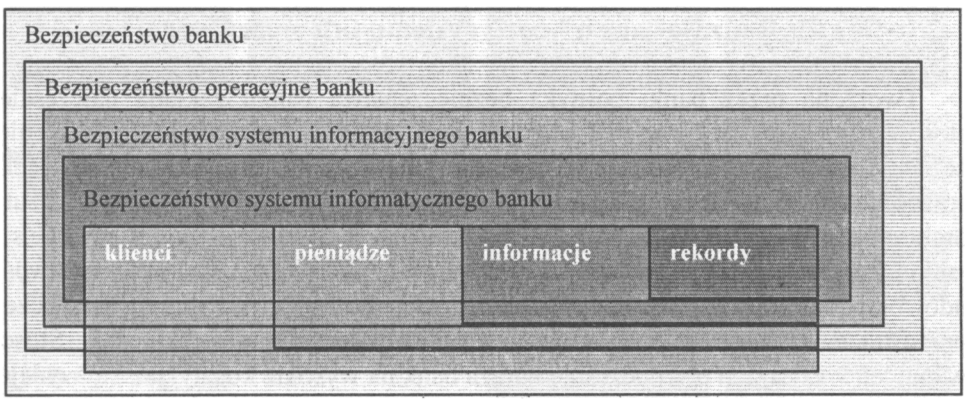
Źródło: opracowanie własne.

Podobnie rzecz ma się z płaszczyzną funkcjonalną. W erze preinformacyjnej poczucie bezpieczeństwa zapewniało rzetelne wykonywanie zleceń klientów. Obecnie to już nie wystarcza. Właściwa realizacja zlecenia musi gwarantować dodatkowo także poufność informacyjną, którą należy rozumieć bardzo szeroko: jako brak możliwości podejrzenia, skopiowania, wykradzenia i użycia danych o prowadzonych przez klientów w bankach rachunkach, jak i o operacjach realizowanych za ich pośrednictwem. Co gorsza, pomimo że nie każde z tych wrogich działań musi oznaczać niebezpieczeństwo, to jest jednak tak przez klientów banku odbierane.

Sytuacje braku pewności odczytuje się jako ryzyko. Dla banków ma ono różne, wzajemnie się warunkujące wymiary. Finansowe rodzaje ryzyka są od dawna znane literaturze i praktyce. Inaczej jest z rodzajami ryzyka o charakterze niefinansowym.

2. Ryzyko operacyjne i informatyczne w polityce bezpieczeństwa informacyjnego banku

Prowadzone przez Bank Rozrachunków Międzynarodowych w Bazylei prace nad stworzeniem nowego, odpowiadającego standardom ery informacyjnej, zbioru wymagań warunkujących bezpieczne zarządzanie bankiem proponują stosowanie nowego podejścia do tworzenia polityki bezpieczeństwa oraz obejmowanego nią ryzyka operacyjnego i informatycznego banku. Pomijając kwestie definicyjne, rodzi się problem współzależności pomiędzy zakresami poszczególnych pojęć. W sposób graficzny przedstawiono to na rys. 3.



Rys. 3. Struktura poszczególnych kategorii ryzyka niefinansowego banku z uwzględnieniem czynników płaszczyzny przedmiotowej

Źródło: opracowanie własne.

Bezpieczeństwo banku to odpowiednik abstrakcyjnej sytuacji opanowania zagrożeń ze strony wszelkich rodzajów ryzyka. Ma ono dwa składniki. Pierwszym jest bezpieczeństwo finansowe, które nie jest przedmiotem zainteresowania niniejszego opracowania. Jest to sytuacja związana z zapewnieniem bezpieczeństwa klientom banku. Drugim jest bezpieczeństwo operacyjne. Jest to sytuacja zapewnienia bezpieczeństwa środkom pieniężnym znajdującym się w dyspozycji banku, a pochodzącym od klientów.

Bezpieczeństwo operacyjne ma także dwa aspekty, z których jeden związany jest z ryzykiem funkcjonowania innych systemów niż informacyjne, a drugi odpowiada ryzyku funkcjonowania systemu informacyjnego banku. Kryterium jego zapewnienia na płaszczyźnie przedmiotowej jest bezpieczeństwo informacji.

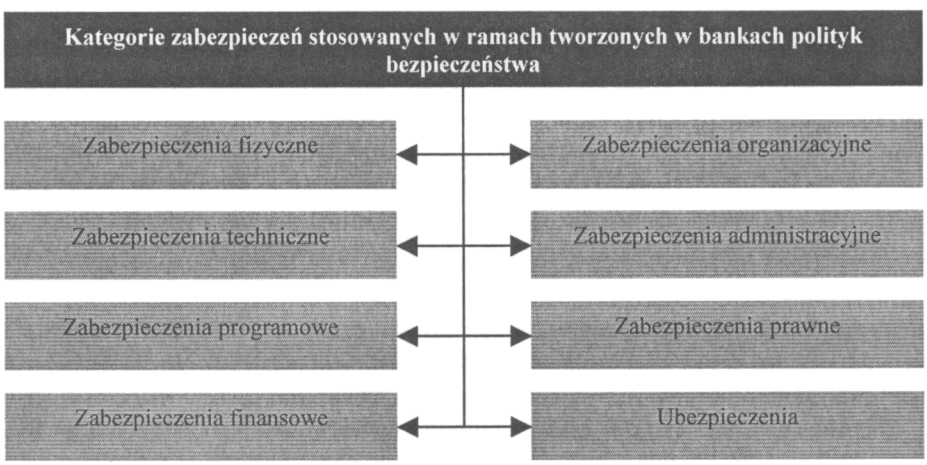
Bezpieczeństwo systemu informacyjnego banku ma znów dwa aspekty. Pierwszy to działania zmierzające do eliminacji zagrożeń ze strony wszelkich składników systemu informacyjnego innych niż systemu informatyczny, a drugi to działania, których celem jest eliminacja zagrożeń wywołanych funkcjonowaniem systemu informatycznego. Na płaszczyźnie przedmiotowej jego kryterium jest zapew-

nienie bezpieczeństwa poszczególnych rekordów (pojedynczych danych zbieranych w trakcie działania banku).

Zaproponowana na rys. 3 hierarchia kategorii postrzegania bezpieczeństwa odzwierciedla wyraźnie spójność zagadnienia. Bezpieczeństwo banku jest ściśle uzależnione od zapewnienia bezpieczeństwa każdego czynnika w wymiarze przedmiotowym, a to jest możliwe tylko w drodze eliminacji zagrożeń bezpieczeństwa każdej z opisywanych kategorii. Rozumując przekornie, można stwierdzić inaczej: że jeżeli nie zapewni się odpowiedniego poziomu bezpieczeństwa dla pojedynczej danej, to nie można być pewnym bezpieczeństwa informacji, pieniędzy i klientów banku.

3. Rodzaje zabezpieczeń systemu informacyjnego

Tworzona przez banki polityka bezpieczeństwa banku zakłada najczęściej stosowanie wszelkich znanych form zabezpieczeń. Można wręcz odnieść wrażenie, że ich stosowanie w komplecie jest atutem konkurencyjnym. Nacisk na kompleksowość wynika z dążenia zarządzających bankami do uchronienia się od zarzutu braku dbałości o bezpieczeństwo. Jak zwykle tego rodzaju strategia nie wydaje się racjonalna, choć należy przyznać, że zapewnia władzom banków możliwość udowodnienia troski o bezpieczeństwo. Wszystkie kategorie form zabezpieczeń przedstawiono na rys. 4. Niektóre z nich się uzupełniają, inne wykluczają. Stosowanie ich wszystkich równocześnie naraża bank na wysokie koszty, jak się wydaje, nie zawsze uzasadnione ekonomicznie. W kwestiach zapewnienia bezpieczeństwa jednak aspekt racjonalności ekonomicznej nie zawsze jest wysuwany na pierwszy plan.

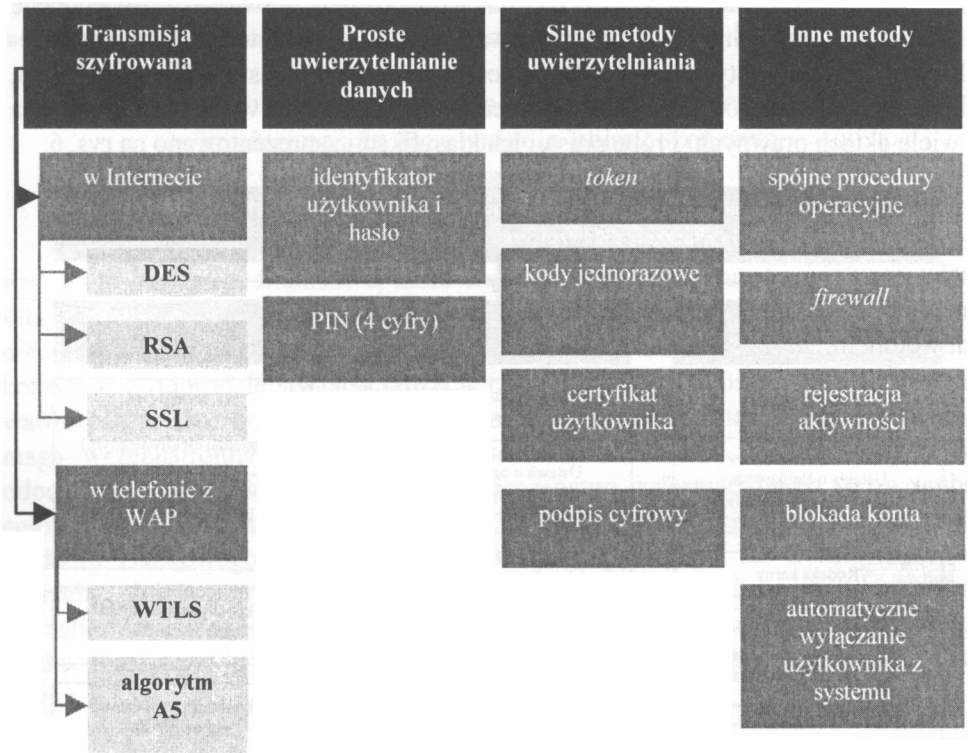


Rys. 4. Kategorie zabezpieczeń stosowanych w ramach tworzonej w bankach polityki bezpieczeństwa

Źródło: opracowanie własne.

Odpowiedź na to pytanie jest możliwa dopiero w świetle wniosków wynikających z rys. 4 i 5. Klienci nie są bezpieczni, jeżeli polityka bezpieczeństwa ich banku uwzględnia tylko zabezpieczenia fizyczne, techniczne i programowe. Konieczne jest bowiem stosowanie także wybranych zabezpieczeń organizacyjnych, prawnych, finansowych i ubezpieczeń.

Duże znaczenie ma w każdej polityce bezpieczeństwa elastyczne jej przystosowywanie do konkretnych niebezpieczeństw zagrażających bankowi i obsługiwanym przez niego klientom [Gadzińska 2004, s. 73-97]. Duże znaczenie dla tej sfery zarządzania bankiem mają także wymagania nadzoru bankowego.



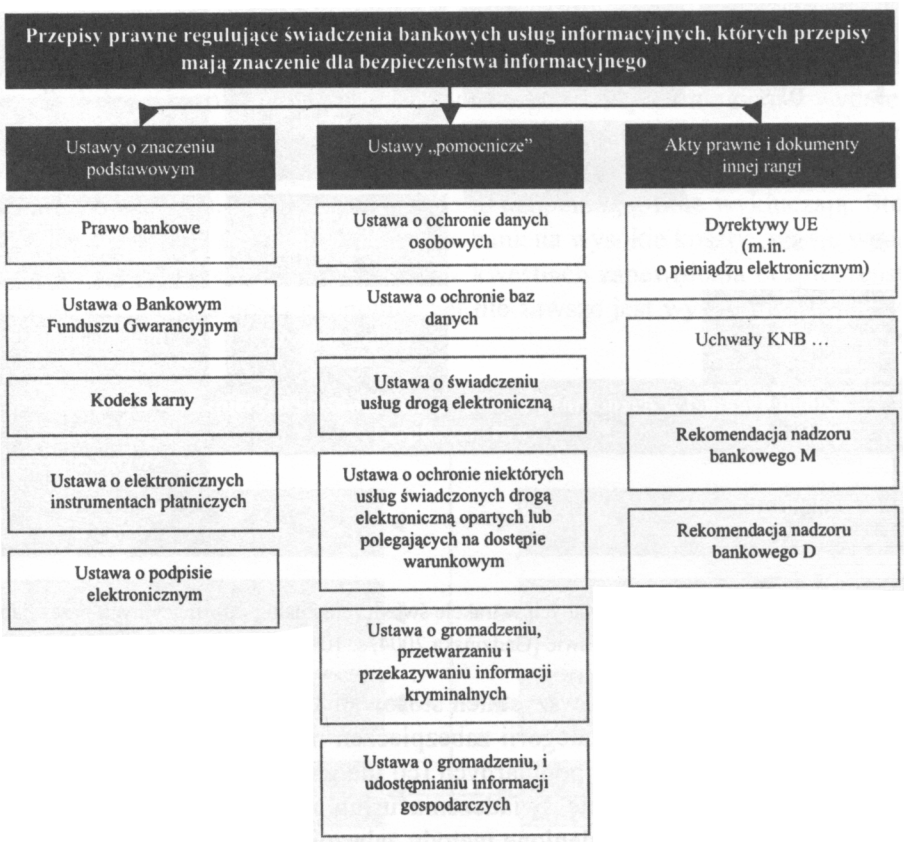
Rys. 5. Rodzaje zabezpieczeń stosowanych w trakcie świadczenia usług informacyjnych przez banki
Źródło: opracowanie własne na podstawie [Gadzińska 2004, s. 109-129].

Szczegółowe wymienienie wszystkich stosowanych w ramach poszczególnych (przedstawionych na rys. 4) kategorii zabezpieczeń metod jest trudne z uwagi na ich liczbę. Zestaw najbardziej popularnych (co nie znaczy, że jest to zestaw kompletny), stosowanych w trakcie świadczenia usług informacyjnych przez banki, przedstawiono na rys. 5. Wymienione metody zabezpieczeń mają charakter fizyczny, techniczny oraz programowy. Użytkownicy serwisów świadczących usługi bankowości elektronicznej są, wbrew obiegowym opiniom, dobrze chronieni. Czy jednak oni i ich pieniądze powierzone bankom są bezpieczne?

Konieczny jest ciągły monitoring zagrożeń, wsparty audytem zabezpieczeń sporządzanym przez zewnętrzne, wyspecjalizowane firmy. Tylko tego rodzaju rozwiązanie zapewnić może obdarzanie stosowanej przez bank polityki bezpieczeństwa koniecznym minimum zaufania.

4. Przepisy prawne dotyczące zapewnienia bezpieczeństwa systemu informacyjnego banku

Szczególnym aspektem tworzonej w bankach polityce bezpieczeństwa jest zabezpieczenie prawne. W Polsce nie ma jednego aktu prawnego poświęconego zagadnieniom zapewnienia bezpieczeństwa w ogóle, a klientom banku w szczególności. Przepisy dotykające kwestii zapewnienia bezpieczeństwa klientom banku, ich pieniędzy oraz informacji i danych zbieranych na ich temat w bankach zawarte są w wielu aktach prawnych. Próbę prostej ich klasyfikacji zaprezentowano na rys. 6.



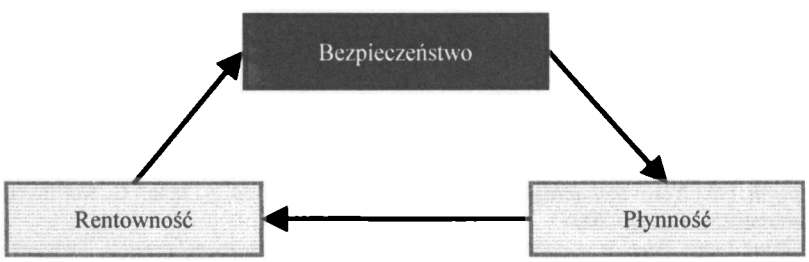
Rys. 6. Klasyfikacja aktów prawnych, których szczegółowe zapisy mają znaczenie dla sfery bezpieczeństwa informacyjnego banku

Źródło: opracowanie własne na podstawie aktów prawnych.

Przedstawiona klasyfikacja ustaw i innych dokumentów prawnych daje wyobrażenie, jak wiele jest przepisów, których treść należy uwzględniać w polityce bezpieczeństwa. Rodzi to trudności interpretacyjne i jest źródłem wielu nieporozumień. Szczególne miejsce przypada wśród tych aktów prawnych uchwałom Komitetu Nadzoru Bankowego (KNB) i rekomendacjom nadzoru bankowego (których autorem jest Główny Inspektor Nadzoru Bankowego). Uchwały KNB są źródłem niezbędnych do respektowania przez banki przepisów prawnych dotyczących głównie sfery zabezpieczeń finansowych i organizacyjnych, a rekomendacje D i M to zbiór „dobrych praktyk" w zakresie zapewnienia bezpieczeństwa systemów informatycznych oraz zarządzania ryzykiem operacyjnym. Dokumenty te uwzględniają wnioski wypływające z „nowej umowy kapitałowej".

5. Zmiany w zarządzaniu bankiem wywołane koniecznością zapewnienia bezpieczeństwa systemu informacyjnego banku

Działalność banków silnie ewoluowała przez szesnaście lat gospodarki rynkowej. Są to instytucje finansowe, które coraz częściej należy utożsamiać z uniwersalnymi pośrednikami finansowymi, które, szeroko wykorzystując zdobycze technologii informacyjnych, stosują w codziennym działaniu *outsourcing*, aby w pełni korzystać z dobrodziejstw specjalizacji [Janc, Kotliński 2002 s. 37-51]. W tych warunkach konieczność zapewnienia bezpieczeństwa informacyjnego banku wymaga wszechstronnych przemian w zarządzaniu bankami, nakierowanych na odpowiednio wysokie uplasowanie bezpieczeństwa informacyjnego w hierarchii celów banku. Służą temu przede wszystkim poszczególne zapisy uchwał Komisji Nadzoru Bankowego oraz rekomendacji nadzorczych D i M. Syntetyzując na potrzeby niniejszego opracowania ich treść, można posłużyć się popularnym na początku lat dziewięćdziesiątych modelem „magicznego" trójkąta decyzyjnego banku. Konieczna jest jednak jego modyfikacja przedstawiona w formie graficznej na rys. 7.



Rys. 7. Postulowana modyfikacja teorii „magicznego" trójkąta decyzyjnego w zarządzaniu bankiem
Źródło: opracowanie własne na podstawie [Kotliński 2003, s. 157-183].

Modyfikacja polega na uczynieniu bezpieczeństwa (w tym także bezpieczeństwa informacyjnego) celem najwyższym, warunkującym realizację pozostałych, w tym przede wszystkim płynności, bez której, z kolei, nie jest możliwe osiągnięcie rentowności. Odpowiednio wysoka rentowność „domyka" trójkąt i umożliwia niezbędne inwestycje w bezpieczeństwo, których celem jest zapewnienie jej na przyszłość. Zadanie dbania o bezpieczeństwo w świetle przytaczanych w tym opracowaniu aktów prawnych przypada najwyższym organom władzy banku – radzie i zarządowi. Aby się z niego wywiązać, muszą korzystać z cieszących się zaufaniem instytucji zewnętrznych, które będą przeprowadzać zewnętrzne audyty zabezpieczeń.

6. Zakończenie

Współczesny bank uzależnił się od stosowanych technologii informacyjnych. Konieczność zapewnienia bezpieczeństwa informacyjnego banku stała się wyzwaniem i celem dążeń dla osób nim zarządzających. Realizacja tego celu wymaga znajomości wszelkich kategorii zabezpieczeń. Niezbędny jest ich racjonalny dobór w zależności od wskazówek monitoringu zagrożeń i wyników zewnętrznego audytu zabezpieczeń. Paradoksem działań podejmowanych dla zapewnienia bezpieczeństwa jest fakt jego abstrakcyjnego charakteru. O tym, jak długo bank jest bezpieczny, decydują przestępcy. Wielkie znaczenie ma wciąż rosnący poziom ich wiedzy i umiejętności. Aby się przed nimi ochronić, pracownicy banku muszą przestrzegać reguł ograniczania ryzyka operacyjnego i informatycznego. W zarządzaniu bankiem prowadzi to do zmiany interpretacji magicznego trójkąta decyzyjnego.

Literatura

Chojecki T., Kotliński G., *Bankowość elektroniczna w działalności banku komercyjnego*, [w:] *Funkcjonowanie współczesnego banku*, red. A. Janc i A. Krymarys-Balcerzak, Akademia Ekonomiczna, Poznań 2004.

Gadzińska M., *Wybrane aspekty polityki bezpieczeństwa informatycznego banku*, [w:] *Nowe technologie we współczesnym banku*, red. A. Janc i G. Kotliński, Akademia Ekonomiczna, Poznań 2004.

Gadzińska M., *Charakterystyka zagrożeń i dobór form zabezpieczeń bankowych systemów informatycznych*, [w:] *Nowe technologie we współczesnym banku*, red. A. Janc i G. Kotliński, Akademia Ekonomiczna, Poznań 2004.

Janc A., *Bank i jego miejsce w pośrednictwie finansowym okresu transformacji*, Twigger, Warszawa 2004.

Janc A., Kotliński G., *Wybrane dylematy polityki zatrudnienia w nowoczesnej instytucji kredytowej na tle zależności między informatyzacją i konkurencyjnością banku*, [w:] *Zastosowania rozwiązań informatycznych w instytucjach finansowych*, red. A. Gospodarowicz, Prace Naukowe Akademii Ekonomicznej nr 954, Wrocław 2002.

Kotliński G., *Zarządzanie ryzykiem utraty płynności banku komercyjnego*, [w:] *Zarządzanie ryzykiem i płynnością banku komercyjnego.* Wydanie 2 zmienione, red. nauk. W. Przybylska-Kapuścińska, Materiały Dydaktyczne nr 134, Akademia Ekonomiczna, Poznań 2003.

SELECTED MANAGERIAL ASPECTS OF PROVIDING BANK'S IT SECURITY

Summary

Nowadays, a contemporary bank fully depends on IT technology. Therefore, it is a real challenge for the Bank's authority to ensure its IT security. The document focuses on the selected modifications in the bank's management resulting from new approach to operational risk. It is included in the documents published by Bank's Supervisory Board as well as in the legal acts put into life. Bank's IT security is a priority to manage all the institutions. The achievement of such a situation requires from each financial institution, especially from the Bank, proper correlation between technical means and financial ones. This is a difficult task because mistakes are not allowed. The outcomes can be extremely serious for an individual bank. Thus, it is important to find general solutions based on the support from institutions in charge.

Dr Grzegorz Kotliński jest adiunktem w Katedrze Bankowości AE w Poznaniu oraz opiekunem naukowym Studenckiego Koła Naukowego Bankowości
e-mail: grzegorz.kotlinski@ae.poznan.pl