

Aleksandra Usik

Uniwersytet Ekonomiczny w Poznaniu

UBEZPIECZENIA POKRYWAJĄCE RYZIKO BANKOWE JAKO METODA OGRANICZANIA SKUTKÓW PRZESTĘPSTW BANKOWYCH

Streszczenie: Przepęstwa bankowe tworzą skomplikowaną strukturę i są trudne do jednoznacznego sklasyfikowania. W niniejszym artykule podzielono je na trzy grupy. Pierwszą stanowią te, w których bank jest sprawcą przestęstwa, w drugiej bank jest ofiarą, w trzeciej zaś jest wykorzystywany do przeprowadzania nielegalnych transakcji. W przypadku gdy bank jest ofiarą, można zastosować środki pozakarne zapobiegające przestęstwom bankowym. Należą do nich zarządzanie ryzykiem operacyjnym oraz ubezpieczenia. Celem artykułu jest opisanie pakietów ubezpieczeń zabezpieczających aktywa i mienie banku przed ryzykiem przestęstw bankowych oraz dokonanie analizy problemów występujących w ich zakresie na polskim rynku.

Słowa kluczowe: ryzyko operacyjne, przestępczość bankowa, ubezpieczenia.

1. Przepęstwa bankowe jako rodzaj ryzyka operacyjnego

Podejmowanie ryzyka jest wpisane w każdą działalność gospodarczą, a zatem również w bankową. Wynika to z tego, że w momencie podejmowania decyzji nie dysponuje się zwykle pełną informacją, poza tym nie sposób trafnie przewidzieć dalszego rozwoju wydarzeń. Trzeba także brać pod uwagę, że posiadana informacja może być błędna lub niekompletna, co także wpływa na ryzykowność działania. W przypadku banków jedną z ważniejszych kategorii ryzyka jest ryzyko operacyjne. Bazylejski Komitet ds. Nadzoru Bankowego definiuje je jako ryzyko bezpośredniej lub pośredniej straty wynikającej z nieadekwatnych i zawodnych procesów wewnętrznych, dotyczących ludzi i systemów lub wynikających ze zdarzeń zewnętrznych [The New Basel Capital... 2001, s.10]. Według Rekomendacji M¹, do kategorii ryzyka operacyjnego zostały zaklasyfikowane przestęstwa bankowe, o których mowa w tym artykule.

Banki ze swej natury należą do instytucji szczególnie narażonych na stanie się ofiarą oszustwa, gdyż poufność ich działań jest stałym elementem świadczonych przez nie usług. Możliwość popełnienia oszustwa zwiększa również fakt, że ich działanie polega bardziej na zmianie zapisów odpowiednich rachunków niż na fizycznym przemieszczaniu pieniędzy. Często przez długi czas nielegalny proceder nie zostaje wykryty, zaś jeśli już zostanie stwierdzony, banki nie przyznają się do

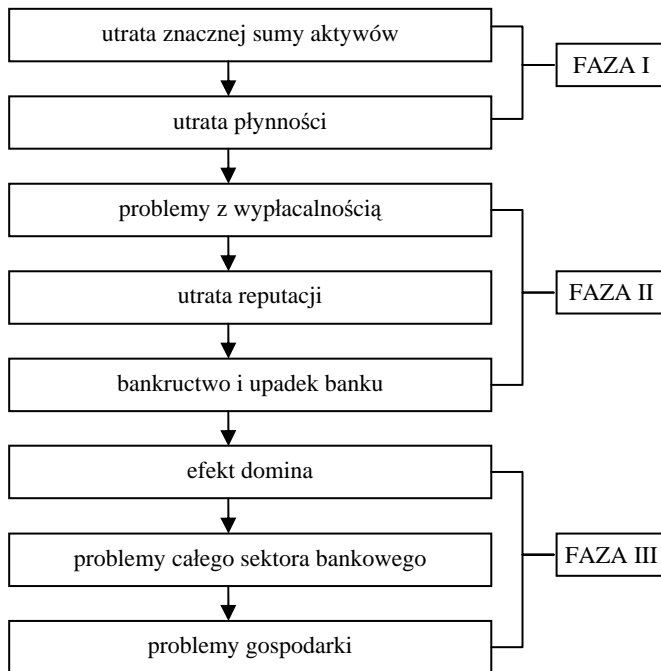
¹ Rekomendację M z 2004 r. opracowano w Wydziale Regulacji Ostrożnościowych Biura Polityki Nadzorczej GINB, Warszawa 2004.

tego, że w ich organizacji zostało popełnione przestępstwo. Nie chcą bowiem narażać się na ryzyko utraty reputacji i konsekwencje z tym związane. Czyny mieszczące się w ramach pojęcia gospodarczej przestępczości bankowej można zdefiniować na podstawie różnych kryteriów. Podejmując próbę dokonania przeglądu podstawowych zagrożeń związanych z prowadzeniem działalności bankowej, ze względu na pozycję banku w trakcie popełniania przestępstwa, wymienia się trzy grupy przypadków [Scheu 1995, s. 74]:

- bank jako sprawca przestępstwa,
- bank jako ofiara,
- bank jako instytucja wykorzystywana do przeprowadzania nielegalnych transakcji.

W pierwszym przypadku bank jest sprawcą. Przestępstwa takie godzą w interesy osób, z którymi bank łączy różne stosunki, najczęściej klientów banku. Natomiast w przypadku drugim bank atakowany jest od wewnątrz przez swoich pracowników o różnym zakresie kompetencji lub z zewnątrz przez osoby trzecie, którymi mogą być jego kredytobiorcy lub usługobiorcy [Górniok 1994, s. 80]. Trzeci przypadek wyodrębniono ze względu na pojawienie się zagrożenia, jakim jest pranie brudnych pieniędzy.

Pojawia się pytanie, dlaczego zapobieganie przestępczości bankowej jest tak ważne, i to nie tylko dla banku, ale także dla całej gospodarki. Aby na nie odpowie-



Rys. 1. Szkody powstałe w wyniku realizacji przestępstwa bankowego

Źródło: opracowanie własne.

dzieć, należy przedstawić ciąg przyczynowo-skutkowy potencjalnych szkód, powstałych w wyniku realizacji przestępstw bankowych (rys. 1).

W pierwszej fazie problem dotyczy tylko banku, wobec którego dopuszczono się czynu zabronionego. W wyniku dokonania przestępstwa bank traci pewną część aktywów. Jeśli suma ta jest znaczna, bank może mieć problemy z płynnością. Szkody powstałe w tej fazie jest najłatwiej naprawić, gdyż zatuszowanie sprawy przestępstwa przed opinią publiczną i szybka reakcja na utratę płynności² sprawiają, że klienci nawet nie wiedzą o problemach banku i wciąż mają do niego zaufanie, w wyniku czego bank może normalnie prosperować. To właśnie dlatego banki, które stały się ofiarą przestępstwa, nie dochodzą swoich praw na drodze sądowej, a każde niepowodzenie utajniają.

Znacznie gorsza sytuacja następuje wtedy, gdy bank zaczyna mieć problemy z wypłacalnością (etap pierwszy fazy drugiej). Klienci już wiedzą, że bank ma jakieś problemy i jego sytuacja jest niepewna. Tracą zaufanie do banku, a ten traci swoją reputację. Następuje masowa wypłata środków z kont, co prowadzi do jeszcze większego pogorszenia sytuacji banku, a ostatecznie do jego bankructwa i upadku. Faza ta jest o tyle niebezpieczna, że zostaje osłabione zaufanie klientów, nie tylko do banku upadającego, ale do wszystkich prosperujących banków w danej gospodarce.

Gdy nastąpi osłabienie pozycji wszystkich banków może dojść do tzw. efektu domina. Upadek jednego banku pociąga za sobą osłabienie pozycji innych banków, co także może przyczynić się do ich upadku [Hałaj 2005, s. 39]. Tak powstaje zagrożenie dla całego sektora bankowego, a w ekstremalnej sytuacji, gdyby wszystkie funkcjonujące banki w gospodarce upadły i nie miałby kto przejąć ich funkcji, zachwiana zostałaby stabilność i rozwój całej gospodarki. Dyskredytuje to wiarygodność państwa na rynkach międzynarodowych. Można już wtedy mówić o kryzysie finansowym. Oczywiście, nie musi to nastąpić, jeżeli państwo, bank centralny czy wreszcie same banki nie pozwolą na sytuacje prowadzące do takich skutków.

2. Wybrane sposoby przeciwdziałania przestępstwom bankowym

Sposobów, które można wykorzystać, aby przeciwdziałać opisanym problemom, jest wiele. Specyfika przestępczości bankowej przejawia się m.in. w tym, iż przeciwdziałanie temu zjawisku obejmuje działania prawne i faktyczne, dlatego środki zapobiegające można podzielić na dwie grupy: wynikające z regulacji o charakterze prawnokarnym (takich jak *Prawo bankowe*, *Kodeks karny*, regulacje Banku Centralnego oraz nadzoru bankowego) oraz środki pozakarne (procedury zarządzania ryzykiem bankowym i ochrony aktywów banku) [Karaźniewicz 2005, s. 221]. Zadanie tych pierwszych sprowadza się do penalizacji w różnych ustawach czynów niebezpiecznych dla gospodarki i instytucji w niej działających. Są one niezbędne w przeciwdziałaniu patologiom ekonomicznym, jednak ich rola nie ma charakteru priory-

² Np. przez wykorzystanie rezerw, pożyczkę od innego banku czy wypłatę odszkodowania itp.

tetowego, lecz jedynie wspomagający. Żadna instytucja, w tym bank, nie może liczyć na to, że nie padnie ofiarą oszustwa tylko dlatego, że jest ono uregulowane w ustawie i podlega sankcji karnej. Zawsze znajdzie się osoba, dla której korzyści z popełnienia czynu zabronionego będą przewyższały ryzyko związane z jego ujawnieniem. Z tego powodu ważną rolę w zapobieganiu przestępczości odgrywają środki pozakarne, które opierają się na właściwym zarządzaniu ryzykiem bankowym, a szczególnie, ze względu na charakter przestępczości, ryzykiem operacyjnym.

Celem zarządzania ryzykiem operacyjnym w banku jest antycypowanie przypadkowych strat i przygotowanie oraz wdrożenie procedur, które pozwolą minimalizować ich występowanie lub ograniczyć znaczenie tych, które już wystąpiły [Vaughan, Vaughan 2003, s. 15]. Mając zidentyfikowane i zmierzone ryzyko operacyjne, na które bank jest narażony, musi on podjąć pewne działania redukujące nadmiar ryzyka. Ma tutaj kilka możliwości, może wybrać strategię aktywną bądź pasywną, skupić się na działaniach profilaktycznych bądź kompensacyjnych. Do podstawowych metod ograniczających niekorzystne skutki ryzyka operacyjnego zalicza się [Cruz 2002, s. 233]:

- aktywne działania mające na celu złagodzenie ryzyka (*risk mitigation*);
- alokację kapitału (*capital allocation*);
- wykup ubezpieczenia (*insurance*).

Pierwsza metoda jest najbardziej oczywistym sposobem zabezpieczenia się banku przed skutkami realizacji ryzyka defraudacji. Stosowanych działań może być bardzo wiele, a ich liczba zależy od pomysłowości osób zarządzających ryzykiem w danym banku i rodzaju zdarzenia, którego skutki chcemy wyeliminować lub złagodzić.

Druga metoda, alokacja kapitału, polega na utrzymywaniu kapitału, który zabezpiecza bank przed skutkami zmienności wyników w następstwie strat operacyjnych [Matkowski 2006, s. 162]. Aby alokacja kapitału była skuteczna, wielkość amortyzującego kapitału musi uwzględniać rzeczywisty poziom ryzyka defraudacji w organizacji. Metoda ta wydaje się skutecznie zabezpieczać ciągłość działalności banku, niestety jej wysoka efektywność jest okupiona wysokimi kosztami, które wynikają z konieczności utrzymywania kapitału w płynnych papierach.

Poprawne zarządzanie ryzykiem w banku oraz stosowanie powyżej opisanych metod może znacznie ograniczyć zagrożenia wynikające z działalności przestępczej, jednak nie wyeliminuje ich całkowicie. Dlatego banki szukają wsparcia na rynku ubezpieczeniowym w celu rozłożenia ryzyka. Należy oczywiście pamiętać, że ubezpieczenie nie może być traktowane jako rozwiązanie alternatywne dla zarządzania ryzykiem. Wprowadzenie jednego elementu nie może rozluźnić dyscypliny w stosowaniu drugiego [Nowak 1999, s. 72]. Oba te procesy powinny być komplementarne.

Oszustwo, rabunek, przestępczość elektroniczna czy pomyłki pracowników to jedne z najgroźniejszych rodzajów ryzyka bankowego³. Można je zabezpieczyć specjalistycznymi produktami oferowanymi przez towarzystwa ubezpieczeń. Wśród

³ Miano najgroźniejszych przypisuje się im z powodu poważnych konsekwencji ich realizacji, którym w skrajnym przypadku jest bankructwo banku.

produktów tych, zabezpieczających majątek banku i środki pieniężne jego klientów, wyróżnia się [Dygas 2008a, s. 43]:

- polisę BBB (*Bankers Blanket Bonds*);
- polisę CC (*Computer Crime*) pokrywającą wszelkie rodzaje ryzyka związane z elektronicznym obrotem i przesyłaniem danych;
- polisę PI (*Professional Indemnity*) dotyczącą roszczeń osób trzecich wobec błędów pracowników;
- polisę D&O (*Directors & Officers*) pokrywającą roszczenia osób trzecich związanych z błędami kadry kierowniczej;
- polisę PC (*Plastic Card*) zabezpieczającą rodzaje ryzyka związane z emisją, fałszowaniem lub utratą kart płatniczych;
- polisę UTP (*Unauthorised Trading Policy*) ubezpieczającą nieautoryzowane transakcje.

Najważniejsza z punktu widzenia przestępczości bankowej, rozumianej jako umyślne działanie na szkodę banku, jest polisa BBB. Jej też zostanie poświęcona kolejna część artykułu.

3. Polisa *Bankers Blanket Bonds*

Polisa BBB ma zabezpieczać aktywa i mienie banku od skutków realizacji takich rodzajów ryzyka bankowego, jak oszustwo, rabunek czy fałszerstwo [Howorth, Lown-des 1999, s. 28]. Ramy umowy dostępne są w ogólnych warunkach danego ubezpieczenia, jednakże ostateczna postać polisy BBB jest różna dla różnych banków ze względu na konieczność dostosowania polisy do indywidualnego profilu ryzyka w danym banku. Zależy ona np. od specyfiki działalności banku, ustawodawstwa kraju, w którym prowadzona jest działalność, czy od wielkości banku, jego struktury i złożoności [Nowak 1999, s. 72]. Przez takie wyspecyfikowanie polisy możliwe jest zapewnienie elastyczności na stale zmieniającym się rynku. Do najczęściej stosowanych klauzul polisy BBB należą [Lloyd's Worldwide..., s. 3]:

- nieuczciwość pracownika;
- miejsce ubezpieczenia;
- przewóz;
- sfalszowane чеки;
- sfalszowane papiery wartościowe;
- sfalszowane pieniądze;
- straty w wyposażeniu biur.

Łatwość dostępu do pieniądza gotówkowego oraz pieniądza w postaci elektronicznej są warunkiem sprzyjającym dla popełniania defraudacji przez pracowników banku, dlatego główną klauzulą ubezpieczeniową polisy BBB jest klauzula nieuczciwości pracownika, zwana także klauzulą sprzeniewierzenia. Ma ona zapewnić pokrycie strat powstałych wskutek nieuczciwości własnego personelu banku. Jednak aby możliwe było zgłoszenie roszczenia, bank musi dokonać identyfikacji pracow-

nika bądź grupy pracowników odpowiedzialnych za zdarzenie oraz udowodnić, że osoby te sprzeniewierzyły mienie banku w wyłącznym celu spowodowania straty banku lub uzyskania nienależnego zysku [Howorth, Lowndes 1999, s. 29]. Zazwyczaj polisa BBB nie pokrywa szkód związanych ze stratami handlowymi powstałymi na skutek np. zaniedbania pracownika, które zostały zatajone, ale nie gwarantowały nienależnego zysku⁴.

Klauzula miejsca ubezpieczenia obejmuje wszystkie straty w lokalu ubezpieczonego powstałe na skutek kradzieży, tajemniczego, niewyjaśnionego zaginięcia, uszkodzenia, zniszczenia lub zaginięcia [Lloyd's Worldwide..., s. 6]. Klauzula ta pokrywa również utratę mienia znajdującego się w posiadaniu klientów wskutek kradzieży na terenie banku [Lloyd's Worldwide ..., s. 6]. Lokale i pomieszczenia biurowe banku muszą być określone we wniosku do polisy w sposób umożliwiający ich jednoznaczną identyfikację [Nowak 1999, s.73]. Dzięki prawidłowemu zarządzaniu ryzykiem bank może ograniczyć tego rodzaju straty przez zastosowanie prostych urządzeń zabezpieczających, takich jak przyciski alarmowe czy nowoczesne kamery. Fakt, że banki zmniejszają poziom przechowywanej gotówki, również wpływa na niższy poziom strat generowanych przez tego typu przestępstwa.

Ryzyko zniszczenia lub utraty walorów pieniężnych podczas przechowywania lub przewozu w pojeździe prowadzonym przez pracownika banku, przewozu w zabezpieczonym i opancerzonym pojeździe pod opieką konwojentów lub wynikającego z uszkodzenia czy utracenia papierów nieprzenoszalnych pokryje klauzula przewozu [Niedałtowski 2008, s. 10-11]. Większość podmiotów oferujących usługi konwojowe zawiera w cenie usługi ubezpieczenie mienia znajdującego się pod ich pieczę, które obejmuje większość zdarzeń. Jednak poleganie wyłącznie na przewoźnikach w przypadku banku jest niewskazane ze względu na jego specyficzną działalność. W przypadku naruszenia warunków polisy lub niezapłacenia składki przez przewoźnika zapewniane pokrycie ubezpieczeniowe traci ważność [Howorth, Lowndes 1999, s. 29]. Polisa typu BBB jest przydatnym dodatkowym zabezpieczeniem w takich okolicznościach.

Kolejne dwie klauzule zapewniają rekompensatę strat banku spowodowanych fałszerstwem [Nowak 1999, s. 73]:

- czeków na skutek sfalszowania podpisu lub oszukańczej zmiany na czeku, poleceniu przelewu, akredytywie itp. lub takich samych czynów na pokwitowaniach odbioru pieniędzy; warunkiem ubezpieczenia jest forma pisemna dokumentów, znajomość ich wyglądu przez pracownika banku oraz dowiedzenie sfalszowania podpisu lub oszukańczej zamiany;
- papierów wartościowych na skutek sfalszowania podpisu, oszukańczej zmiany, podrobienia, utracenia lub kradzieży z zastrzeżeniem formy pisemnej papierów

⁴ Przykładem straty handlowej jest umyślne naruszenie przez pracownika wytycznych działania, a następnie próba ukrycia strat. Zdarzyło się tak w przypadku Nicka Leeson, pracownika Barings Banku, który przez kilka miesięcy nadużywał zaufania przełożonych. W konsekwencji jego działanie było powodem upadku banku. Zob. [Leeson 1997].

wartościowych oraz znajomości ich wyglądu przez pracownika banku, ponadto zakłada się, że podrobiony papier jest imitacją ładną podobną do oryginału.

Ryzyko fałszerstw jest powszechne, jednakże dzięki prawidłowemu zarządzaniu ryzykiem i odpowiedniemu przeszkoleniu personelu możliwe jest znaczne ograniczenie tego zagrożenia. Z ryzykiem fałszerstw związana jest także następująca klauzula ubezpieczeniowa polisy BBB, która dotyczy przyjęcia w dobrej wierze, podczas prowadzenia rutynowej działalności, sfałszowanych pieniędzy [Nowak 1999, s. 73].

Ostatnia z wymienionych klauzul zapewnia pokrycie w przypadku uszkodzenia lokalu lub jego wyposażenia wskutek napadu, włamania lub innej próby tego rodzaju [Howorth, Lowndes 1999, s. 30]. W wielu przypadkach przestępcy po wdarciu się do pomieszczeń bankowych dewastują je, uszkodzają sprzęt biurowy, sejfy i skarbcie. Wymiana takiego sprzętu jest droga, dlatego także stanowi część ubezpieczenia.

W zależności od faktycznych potrzeb danego banku klauzule te mogą być stosowane wybiórczo lub dowolnie łączone, a odpowiadające im limity odpowiedzialności ubezpieczyciela ustalane odrębnie w wysokości odpowiadającej realnym zagrożeniom i ich możliwym rzeczywistym skutkom [Holly 2002, s. 20]. Ważne jest, aby zwrócić uwagę na wyłączenia do klauzul, gdyż może okazać się, że bank zapłaci wysoką składkę, a zaistniała szkoda będzie wyłączona z zakresu ubezpieczenia. Przykładem jest tu definicja pracownika używana przez niektórych ubezpieczycieli, którzy wykluczają z niej kierowników nawet najniższego szczebla [Dygas 2008b, s. 23]. Oznacza to, że bank jest chroniony, jeśli okradnie go kasjerka, jednak jeśli czynu tego dopuści się jej przełożony, bank nie będzie już objęty ochroną ubezpieczeniową. Warto więc zwrócić uwagę na zapisy i definicje zawarte w ogólnych warunkach ubezpieczenia.

4. Pozostałe polisy pokrywające ryzyko przestępstw bankowych

Polisa BBB pokrywa wiele rodzajów ryzyka, których realizacja wiąże się z popełnieniem przestępstw bankowych. Jednakże należy uwzględnić także inne polisy oferowane przez towarzystwa ubezpieczeniowe, które mogą zabezpieczać bank przed negatywnymi skutkami przestępczości bankowej. Są nimi polisa CC oraz polisa PC. Razem z polisą BBB stanowią one kompleksowe zabezpieczenie mienia bankowego.

Standardowa polisa BBB nie zapewnia rekompensaty strat powstałych w wyniku przestępczości komputerowej, chyba że straty te zostały spowodowane przez pracownika banku i podlegają klauzuli pierwszej o nieuczciwości pracownika. Pokrycie strat z tytułu ataku spamów i wirusów komputerowych oraz wydatków dotyczących weryfikacji i odtwarzania danych czy też skutków phishingu zapewni polisa CC. Problemem ze stratami powstałymi wskutek przestępstw komputerowych jest trudność dowiedzenia ich przyczyn. Specyficzny zakres i formułę tego ubezpieczenia zawiera tab. 1.

Straty spowodowane przestępstwami komputerowymi stają się coraz powszechniejsze. W przeciwieństwie do innych przestępstw nie ma dla nich granic narodo-

Tabela 1. Zakres polisy CC

Klauzula	Charakterystyka
1) ubezpieczenie systemów komputerowych	asekuruje oszukańcze wprowadzenie lub zniszczenie danych i związanych z tym strat, sprawca musi osiągnąć zysk lub spowodować stratę dla ubezpieczonego
2) ubezpieczenie działalności biura obsługi banku	pokrywa te same zdarzenia co klauzula 1, ale w aspekcie odpowiedzialności prawnej w stosunku do klientów
3) ubezpieczenie elektronicznych instrukcji komputerowych	zapewnia pokrycie ubezpieczeniowe wypłaty środków oparte na oszukańczych instrukcjach elektronicznych
4) ubezpieczenie danych i nośników elektronicznych	pokrywa straty spowodowane rozmyślnym zniszczeniem danych lub nośników przechowywanych w systemie komputerowym lub w biurze obsługi w formie elektronicznej lub fizycznej
5) ubezpieczenie od wirusów komputerowych	ubezpiecza straty środków finansowych lub mienia oraz koszty rzeczywistego zniszczenia danych na skutek działania wirusa komputerowego
6) ubezpieczenie komunikacji elektronicznej	pokrywa zdarzenia z klauzuli 1, ale na skutek oszukańczej instrukcji skierowanej do systemu komputerowego lub terminala komunikacyjnego ubezpieczonego
7) ubezpieczenie transmisji elektronicznej	działa w kierunku odwrotnym niż klauzula 6 i dotyczy odpowiedzialności prawnej ubezpieczonego w stosunku do klienta, który oparł się na oszukańczych transmisjach elektronicznych
8) ubezpieczenie elektronicznych papierów wartościowych	podobnie jak w klauzuli 6, z tym że jest związana z obrotem papierów wartościowych, więc ubezpiecza się odpowiedzialność prawną ubezpieczonego względem centralnej instytucji depozytowej
9) ubezpieczenie sfalszowanego faksu	pokrywa szkody będące skutkiem zastosowania się ubezpieczonego do oszukańczych instrukcji przesłanych faksem
10) ubezpieczenie instrukcji wydawanych przez telefon	podobnie jak w klauzuli 9, z tym że dotyczy instrukcji wydawanych telefonicznie
11) ubezpieczenie wydatków z tytułu weryfikacji i odtwarzania danych	zapewnia pokrycie opłaconych strat z tytułu kosztów weryfikacji, odtworzenia lub usunięcia elektronicznych instrukcji

Źródło: opracowanie własne na podstawie [Holly 2002, s. 21; Nowak 1999, s. 73; Howorth, Lowndes 1999, s. 30-31].

wych, a elektroniczna postać pieniądza przyczynia się do zwiększenia wartości szkód. Dodatkowo oferowane usługi bankowości elektronicznej zwiększają potencjalne zagrożenie ze strony przestępców komputerowych. Polisa CC skutecznie transferuje ryzyko na towarzystwa ubezpieczeniowe, zabezpieczając w ten sposób aktywa banku i klientów.

Kolejną sferą ryzyka bankowego, którą można ubezpieczyć i na którą należy zwrócić uwagę, jest ryzyko związane z emisją i korzystaniem z kart płatniczych.

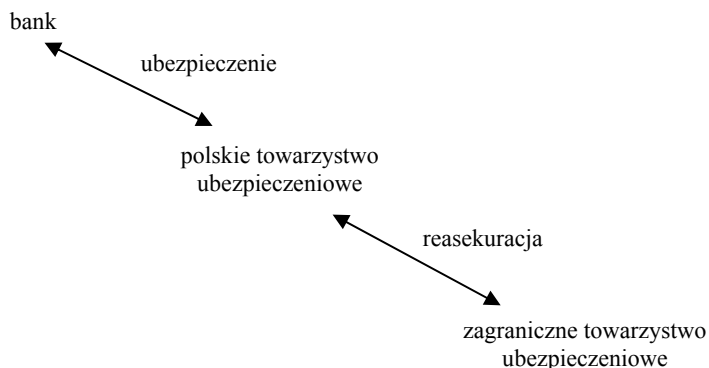
Rosnąca liczba kart bankowych oraz placówek je akceptujących sprawia, że pojawiają się osoby zainteresowane wyłudzeniem pieniędzy przez podrobienie lub fałszowanie kart. Ten rodzaj ryzyka pokrywa polisa PC. Dobrze skonstruowana pozwala zabezpieczyć straty spowodowane realizacją transakcji [Holly 2002, s. 23]:

- kartami sfałszowanymi;
- kartami podrobionymi lub nieuczciwie zmienionymi;
- kartami zgubionymi lub skradzionymi.

Przedstawiony pakiet polis bankowych zapewnia skuteczny transfer większości rodzajów ryzyka związanych z przestępstwami w sektorze bankowym. Mimo to, produkty te nie są zbyt rozpowszechnione na rynku polskim. Powstaje pytanie, w jakim stopniu wynika to ze swoistych uwarunkowań jego funkcjonowania, a w jakim – ze specyfikacji poszczególnych polis przez zakłady ubezpieczeniowe.

5. Problemy na polskim rynku ubezpieczeń przestępstw bankowych

Powody niewielkiego zainteresowania w Polsce ubezpieczeniami przestępstw bankowych są zróżnicowane. Przede wszystkim, należy wskazać, iż banki posiadające zagranicznego akcjonariusza są ubezpieczone od tego rodzaju ryzyka za granicą [Niedałtowski 2008, s. 11]. Tymczasem takie banki dominują w polskim systemie bankowym. Innym powodem jest niewielka podaż ubezpieczeń bankowych oferowanych przez polskie zakłady ubezpieczeń [Broda 1999, s. 33]. Nie wszystkie towarzystwa ubezpieczeniowe mogą oferować skomplikowane produkty przeznaczone dla wąskiej i wymagającej grupy odbiorców, jakimi są banki. Pierwsze polisy bankowe zostały opracowane dla polskiego rynku przez firmy brokerskie, a zawieranie takich umów dokonywało się najczęściej przez negocjowanie i uzgadnianie warunków w polskich towarzystwach reasekurowanych bezpośrednio za granicą (rys. 2) [Broda 1999, s. 33].



Rys. 2. Powiązania między instytucjami zabezpieczającymi ryzyko bankowe

Źródło: opracowanie własne na podstawie [Broda 1999, s. 33].

To właśnie z zagraniczną reasekuracją wiążą się kolejne problemy polskiego rynku ubezpieczeń bankowych. Przełożenie zagranicznych zasad umów ubezpieczeń bankowych na uwarunkowania polskie znacznie je komplikuje. Po pierwsze, powstaje problem natury językowej, gdyż nazewnictwo i charakter wielu instrumentów bankowych w Polsce i za granicą mogą się znacznie różnić [Broda 1999, s. 34]. Po drugie, polski system prawno-ekonomiczny nie pozwala na zastosowanie wszystkich rozwiązań stosowanych za granicą. Przykładem może być stosowana w Polsce reguła *loss occurrence* (wystąpienia szkody), podczas gdy za granicą stosuje się bazę *claims made* polegającą na ochronie ubezpieczeniowej zdarzeń, które zostały odkryte i zgłoszone w okresie obowiązywania polisy [Nowak 1999, s. 74]. Po trzecie, polskie towarzystwa ubezpieczeniowe w ramach zapewnienia sobie marginesu bezpieczeństwa często ograniczają swoje usługi tylko do niektórych klauzul polisy głównej lub stosują indywidualne wyłączenia do klauzul⁵, co stwarza problem rozbieżności ochrony ubezpieczeniowej polskiego towarzystwa ubezpieczeniowego i jego zagranicznego reasekuranta [Broda 1999, s. 34].

Podsumowując, można stwierdzić, że przedstawiony pakiet ubezpieczeń stanowi skuteczne zabezpieczenie aktywów i mienia banku przed ryzykiem przestępstw bankowych. Należy jednak pamiętać, że aby efektywnie chronić bank przed realizacją tych rodzajów ryzyka nie wystarczy samo ich ubezpieczenie. Głównym czynnikiem profilaktycznym ograniczającym przestępczość w banku jest prawidłowe zarządzanie ryzykiem bankowym. Ubezpieczenie powinno być traktowane jedynie jako dodatek, który w przypadku realizacji ryzyka rekompensuje powstałe szkody.

Literatura

- Broda M., *Polskie początki*, „Bank” 1999 nr 2.
- Cruz M.G., *Modeling, Measuring and Hedging Operational Risk*, John Wiley & Sons, New York 2002.
- Dygas M., *Banki pod parasolem*, „Gazeta Bankowa” 2008a nr 24.
- Dygas M., *Polisy dla banków*, „Gazeta Bankowa” 2008b nr 10.
- Górniok O., *Przestępczość gospodarcza i jej zwalczanie*, PWN, Warszawa 1994.
- Hałaj G., *Badanie efektu domina w polskim systemie bankowym*, „Bank i Kredyt” 2005 nr 10.
- Holly R., *Ubezpieczenie w strategii bezpieczeństwa i zarządzania ryzykami banku*, Związek Banków Polskich, Warszawa 2002.
- Howorth D., Lowndes M., *Klauzula na każdą okoliczność*, „Bank” 1999 nr 2.
- Karaźniewicz J., *Bankowe oszustwo kredytowe. Aspekty normatywne, kryminologiczne i polityczno-kryminalne*, Dom Organizatora, Toruń 2005.
- Leeson N., *Łajdak na giełdzie*, Wydawnictwo Finansowe WIG-Press, Warszawa 1997.
- Lloyd’s Worldwide Bankers’s Policy, Lloyd’s Policy Signing Office General Manager, WBP NMA 2626 (27/1/94) Form approved by Lloyd’s Underwriters’ Non-Marine Association.
- Matkowski P., *Zarządzanie ryzykiem operacyjnym*, Wolters Kluwer, Kraków 2006.
- Niedałtowski L., *Specjalnie dla banków*, „Miesięcznik Ubezpieczeniowy” 2008 nr 5.

⁵ Przykładem jest wspomniana już specyficzna definicja pracownika.

- Nowak C., *Ochrona ubezpieczeniowa wybranych ryzyk bankowych*, „Wiadomości Ubezpieczeniowe” 1999 nr 5-6.
- Rekomendacja M z 2004 r. opracowana w Wydziale Regulacji Ostrożnościowych Biura Polityki Nadzorczej GINB, Warszawa 2004.
- Scheu U., *Prawnokarna kontrola rynku kapitałowego i systemu bankowego – doświadczenia niemieckie*, [w:] *Przestępczość gospodarcza. Doświadczenia europejskie i amerykańskie*, red. A. Siemaszko, Oficyna Naukowa, Warszawa 1995.
- The New Basel Capital Accord-an Explanatory Note, Annex 2, Basle Committee on Banking Supervision, January 2001.
- Vaughan E., Vaughan T., *Fundamentals of Risk and Insurance*, John Wiley&Sons, New York 2003.

INSURANCE POLICIES COVERING BANKING RISK AS THE METHOD OF REDUCING THE BANK FRAUDS' IMPACT

Summary: Bank frauds form a complicated structure and they are difficult to be classified explicitly. In this article they are divided into three groups. The first one consists of offences in which a bank is a perpetrator, in the second group a bank is a victim whereas in the third – it is used to carry out a transaction. In the case of a bank being a victim there are off-punitive means that prevent bank frauds. Such means include operational risk management and insurance. The article focuses on insurance packages that protect bank assets and their property against the risk of bank fraud. The packages aim to cover emerged losses. Apart from presenting the spectrum of particular packages the author analyzes the problem of bank risk on the Polish insurance market.