

**Wojciech Stawski\***

## **Audyt Banków Spółdzielczych w zakresie bezpieczeństwa związanego z zagrożeniami kryminalnymi.**

Bezpieczeństwo jest wartością samą w sobie. Należy ono do elementarnych potrzeb człowieka. Wartość ta rozciąga się na wszystkie dziedziny ludzkiej aktywności, między innymi na sferę zawodową. Bezpieczeństwo biznesu jest warunkiem *sine qua non* każdej działalności gospodarczej. Jednak aktywność gospodarcza niesie za sobą większe lub mniejsze ryzyko.

Od takiego ryzyka nie są wolne banki. Bazylejski Komitet ds. Nadzoru Bankowego zdefiniował ryzyko operacyjne jako ryzyko wynikające z wszelkiego rodzaju błędów ludzkich lub błędów spowodowanych przez wykorzystywane środki techniczne<sup>1</sup>. Komisja Nadzoru Bankowego, działając na podstawie art.137 pkt 5 ustawy – Prawo bankowe, wydała „Rekomendację M dotyczącą zarządzania ryzykiem operacyjnym”<sup>2</sup>, której treści korespondują z tekstem „Zasad Dobrej Praktyki w Zakresie Zarządzania i Nadzoru nad Ryzykiem Operacyjnym”, ogłoszonym w lutym 2003 r przez Bazylejski Komitet ds. Nadzoru Bankowego.

Zgodnie z definicją zawartą w przywołanej rekomendacji, **ryzyko operacyjne należy rozumieć jako ryzyko straty wynikające z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów technicznych lub zdarzeń zewnętrznych.**

W banku powinien być opracowany system zarządzania ryzykiem operacyjnym.

Omawiany dokument Komisji Nadzoru Bankowego formułuje szereg wytycznych i postulatów dla władz banku w zakresie ryzyka operacyjnego, między innymi:

- członkowie organów banku – rady nadzorczej i zarządu banku – powinni być świadomi ważnych aspektów ryzyka operacyjnego w banku, jako odrębnego i podlegającego zarządzaniu rodzaju ryzyka i powinni znać profil ryzyka wynikającego z działalności banku,
- rada nadzorcza powinna zatwierdzać (akceptować) opracowane przez zarząd założenia strategii prowadzenia działalności, uwzględniającej występowanie ryzyka operacyjnego, określającej w szczególności ogólne zasady zarządzania tym ryzykiem oraz okresowo oceniać realizację przyjętej strategii,
- kontrola i ocena systemu zarządzania ryzykiem operacyjnym oraz jego regularne przeglądy powinny być dokonywane przez komórkę audytu wewnętrznego, niezależną pod względem

---

1 Basle Committee on Banking Supervision - „Operational Risk Management” - wrzesień 1998 r.

2 Komisja Nadzoru Bankowego - Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym – Warszawa, 2004 r.

operacyjnym i zatrudniającą kompetentny, odpowiednio wyszkolony personel.

Jednym z elementów zarządzania ryzykiem operacyjnym jest bieżące monitorowanie zagrożeń oraz okresowa ocena adekwatności działań organizacyjnych pozwalających na ograniczenie tego ryzyka. Istotną rolę w tym procesie ma audyt wewnętrzny. Zgodnie z rekomendacją KNB, komórka organizacyjna zajmująca się tym zagadnieniem powinna spełniać jednocześnie następujące warunki:

- być niezależną organizacyjnie wobec ocenianych jednostek organizacyjnych,
- zatrudniać kompetentnych i wyszkolonych w zakresie prowadzonego audytu pracowników,
- nie wypełniać bezpośrednio funkcji zarządzania ryzykiem.

Rekomendacja definiuje i systematyzuje kategorie siedmiu zdarzeń związanych z działalnością banku, które mogą skutkować wystąpieniem strat finansowych:

1. oszustwo wewnętrzne,
2. oszustwo zewnętrzne,
3. praktyka kadrowa i bezpieczeństwo pracy,
4. klienci, produkty i praktyka biznesowa,
5. uszkodzenia aktywów,
6. zakłócenia działalności i błędy systemów,
7. dokonywanie transakcji, dostawa oraz zarządzanie procesami.

Pośród wymienionych zdarzeń, podlegających ryzyku operacyjnemu, trzy dotyczą zagrożeń kryminalnych (z wyłączeniem przestępstw intelektualnych):

- oszustwo wewnętrzne (termin nie do końca obejmujący istotę zagrożenia, wynikający prawdopodobnie z niedoskonałości tłumaczenia)- obejmujące przykładowe zdarzenia operacyjne takie jak: kradzież, wymuszenie i rabunek,
- oszustwo zewnętrzne - obejmujące przykładowe zdarzenia operacyjne takie jak kradzież i rabunek ,
- uszkodzenia aktywów - obejmujące przykładowe zdarzenia operacyjne takie jak straty wynikające z działalności terrorystycznej, wandalizmu.

Duże banki organizacyjnie przygotowane są do spełniania zadań związanych z monitorowaniem wymienionych zagrożeń oraz oceny podejmowanych działań, pozwalających na ograniczenie wystąpienia ryzyk. Tworzone są komórki bezpieczeństwa do bieżącego monitorowania zagrożeń i kreowania polityki bezpieczeństwa banku, oraz zespoły audytu wewnętrznego. Takie banki stać na zatrudnienie (i racjonalne wykorzystanie) w wymienionych komórkach organizacyjnych wykwalifikowanych pracowników, przygotowanych do wypełniania

postawionych zadań.

Nieco inaczej sytuacja przedstawia się w bankach spółdzielczych, gdzie stosunkowo spłaszczona struktura nie pozwala na stworzenie komórek audytu wewnętrznego, stale zatrudniających wyspecjalizowanych pracowników, nie wypełniających, jak tego wymaga rekomendacja, bezpośrednio funkcji zarządzania ryzykiem. W niektórych bankach spółdzielczych funkcjonują etaty obsadzone przez pracowników posiadających niezbędną wiedzę w przedmiocie ochrony mienia, np. na stanowiskach szefów ochrony. Z uwagi na wypełnianie przez nich codziennych zadań z zakresu ochrony, nie można ich wiedzy wykorzystać do audytu wewnętrznego w tym zakresie. Musieliby oceniać swoją pracę, co wyklucza obiektywizm.

Zasadnym i racjonalnym rozwiązaniem w tym zakresie wydaje się więc zlecenie przeprowadzenia audytu zewnętrznemu podmiotowi.

Audyt powinien obejmować następujące zagadnienia:

1. Zabezpieczenia organizacyjne.

Do tej grupy należy zaliczyć wszystkie działania organizacyjno-taktyczne oraz prawne, kształtujące politykę bezpieczeństwa w chronionym obiekcie. Do działań organizacyjno-taktycznych należy zaliczyć plany ochrony (lub inne dokumenty o podobnym charakterze.

Ocenie podlega:

- kompletność planu,
- zgodność z obowiązującymi normami prawnymi,
- adekwatność do zagrożeń,
- aktualność,
- wykonawstwo.

Doświadczenia pokazują, że dokumenty te w wielu przypadkach mogą być nieaktualne, w stosunku do faktycznie podejmowanych działań w zakresie ochrony fizycznej i zabezpieczenia technicznego, oraz pojawiających się nowych zagrożeń.

Do działań prawnych należy zaliczyć:

- przepisy wewnętrzne regulujące zasady bezpieczeństwa,
- umowy z podmiotami zewnętrznymi realizującymi zadania ochronne,
- polisy ubezpieczeniowe.

W wielu przypadkach treść instrukcji regulujących zasady bezpieczeństwa może w praktyce zagrażać życiu i zdrowiu pracowników banku i klientów. Analiza treści wielu umów z podmiotami świadczącymi usługi w zakresie ochrony mienia wskazuje, że dokumenty te zabezpieczają głównie interesy wykonawcy .

## 2. Ochrona fizyczna.

W praktyce nie występują obiekty bankowe, które nie są chronione przez pracowników ochrony fizycznej. Czasami jest to ochrona wykonywana przez własnych pracowników w postaci wewnętrznej służby ochrony. Częściej jest to ochrona stała w obiekcie, wykonywana przez koncesjonowany podmiot zewnętrzny. Najczęściej ochrona ma charakter doraźny, w postaci tzw. „grup interwencyjnych”. Prawie zawsze banki korzystają z usług Stacji Monitorowania (Alarmowego Centrum Odbiorczego). Przedmiotem audytu w zakresie ochrony fizycznej jest ocena:

- faktycznego wykonawstwa zadań w świetle obowiązujących przepisów prawa,
- zgodności wykonawstwa zadań z planem ochrony oraz warunkami umowy,
- stosowanej taktyki w kontekście bezpieczeństwa personelu banku i jego klientów.

Niestety w wielu przypadkach pozbawione kontroli służby ochrony nie „grzeszą” profesjonalizmem, a ich działania w sytuacjach kryzysowych mogą przynieść odwrotny skutek od zakładanego.

## 3. Zabezpieczenia techniczne.

Przedmiotem audytu jest:

- zgodność zastosowanych urządzeń zabezpieczenia technicznego z obowiązującymi przepisami i normami technicznymi,
- sprawność urządzeń,
- adekwatność do zagrożeń,
- wykonawstwo obowiązków w zakresie konserwacji zainstalowanego sprzętu.

Wynik audytu pozwala na ocenę, czy podejmowane działania organizacyjne, fizyczne i techniczne:

- odpowiadają zagrożeniom,
- nie naruszają interesów banku,
- są optymalnie wykorzystywane.

Wiedza uzyskana z audytu może posłużyć do określenia zakresu koniecznych korekt w systemie bezpieczeństwa oraz wykreować strategię bezpieczeństwa pozwalającego na obniżenie ryzyka operacyjnego w kategoriach będących przedmiotem audytu.

*\* Autor opracowania jest pełnomocnikiem w Spółce NOSTRA zajmującej się doradztwem bezpieczeństwa.*