PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1068 — 2005
Zastosowania rozwiązań informatycznych w bankach spółdzielczych

Dariusz Wawrzyniak
Akademia Ekonomiczna we Wrocławiu

RYZYKO INFORMATYCZNE W DZIAŁALNOŚCI BANKOWEJ

Ryzyko jest związane z każdym przejawem działalności gospodarczej. W zależności od charakteru tej działalności różne jednak znaczenia są przypisywane poszczególnym rodzajom ryzyka. Specyfika działalności bankowej – wynikająca zarówno z uwarunkowań prawnych, jak i z praktyki biznesowej – wymaga istnienia pewnego wspólnego mianownika zarządzania wszystkimi rodzajami ryzyka, wśród nich także ryzykiem informatycznym. Co więcej, złożoność technologiczna i funkcjonalna rozwiązań informatycznych stosowanych w bankowości oraz waga przetwarzanych w tych systemach informacji nadają problematyce zarządzania ryzykiem informatycznym istotnego dla funkcjonowania instytucji bankowych znaczenia. Artykuł niniejszy przedstawia ryzyko informatyczne w bankowości w ogólnym zarysie, nieco więcej miejsca poświęcając problematyce zagrożeń systemów bankowości elektronicznej.

W klasycznym ujęciu w ramach ryzyka bankowego wyróżnia się ryzyko kredytowe, płynności, rynkowe, zmian systemowych oraz ryzyko niefinansowe, określane także jako ryzyko operacyjne.

Problematyka ryzyka operacyjnego jest przedmiotem m.in. prac regulacyjnych Komitetu Bazylejskiego, który w swoich dokumentach zdefiniował je jako „ryzyko strat w wyniku niewłaściwego lub błędnego działania procesu, ludzi i systemów lub wpływu wydarzeń wewnętrznych" [*Operational...* 2001]. W dokumentach Komitetu można znaleźć także ramowy podział ryzyka operacyjnego na następujące rodzaje:

- ryzyko oszustwa ze strony pracowników,
- ryzyko oszustwa pochodzące z zewnątrz,
- ryzyko w zakresie zasad zatrudniania i BHP,
- ryzyko w zakresie zasad pracy z klientami i produktami,
- ryzyko szkód zasobów materialnych,

- ryzyko zakłócenia prowadzenia biznesu i niesprawności systemu,
- ryzyko zarządzania wykonywaniem zadań.

Komitet podjął także próbę nieco bardziej szczegółowego odniesienia się do omawianej problematyki w kontekście bankowości elektronicznej. Zasady zarządzania ryzykiem w bankowości elektronicznej [*Risk*... 2003] to dokument będący swego rodzaju zbiorem ogólnych rekomendacji Komitetu, dotyczących tego obszaru działalności bankowej, który bezpośrednio wpływa na szeroko rozumiane bezpieczeństwo systemów bankowości elektronicznej. W dokumencie sformułowanych zostało m.in. 14 zasad zarządzania ryzykiem, które wyznaczają cele działań ukierunkowanych na zapewnienie optymalnego poziomu bezpieczeństwa konkretnych rozwiązań. Zasady te podzielono na trzy grupy (rys.1).

A. Kontrola ze strony Rady i Zarządu
1. Efektywna kontrola bankowości elektronicznej przez kierownictwo.
2. Ustanowienie wszechstronnego procesu kontroli bezpieczeństwa.
3. Wszechstronne zasady należytej staranności i kontrolowanie przez kierownictwo procesu zlecania usług na zewnątrz oraz innych rodzajów uzależnień od stron trzecich.

B. Mechanizmy kontroli bezpieczeństwa
1. Sprawdzenie tożsamości klientów bankowości elektronicznej.
2. Uniemożliwienie negowania dokonanych transakcji oraz odpowiedzialność za transakcje bankowości elektronicznej.
3. Odpowiednie środki zapewniające podział obowiązków.
4. Właściwe mechanizmy kontroli upoważnień w ramach systemów, baz danych i aplikacji bankowości elektronicznej.
5. Rzetelność danych dotyczących transakcji, zapisów i informacji z zakresu bankowości elektronicznej.
6. Ustanowienie jasno określonych ścieżek audytu dla transakcji bankowości elektronicznej.
7. Poufność podstawowych informacji bankowych.

C. Zarządzanie ryzykiem prawnym i ryzykiem reputacji.
1. Odpowiednia sprawozdawczość dotycząca usług bankowości elektronicznej.
2. Poufność danych o klientach.
3. Pojemność systemu, zapewnienia ciągłości działalności i planowanie awaryjne w celu zapewnienia dostępności systemów i usług bankowości elektronicznej.
4. Plany reagowania na incydenty.

Rys. 1. Zasady zarządzania ryzykiem w bankowości elektronicznej

Źródło: [*Risk*... 2003].

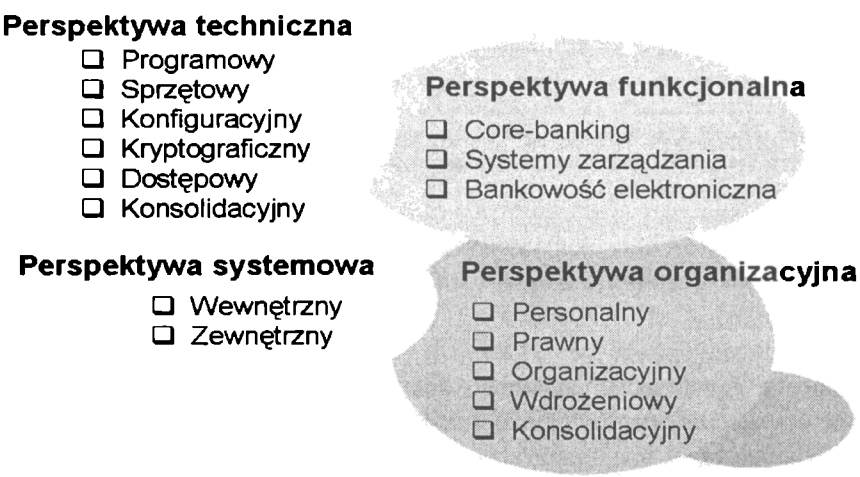
Mimo że zawartość omawianego dokumentu pozostawia wiele do życzenia, głównie w warstwie terminologicznej, stanowi on podstawę zaleceń i rekomendacji publikowanych przez banki centralne w poszczególnych krajach Unii Europejskiej, także w Polsce (zob. np. [*Rekomendacja D* 2002]).

Zalecenia Komitetu, pochodne im rekomendacje Narodowego Banku Polskiego oraz praktyka bankowa nakazują wyróżniać w ramach ryzyka operacyjnego ryzyko or-

ganizacyjne, personalne, otoczenia i informatyczne. Powszechnie uważane za fundamentalny element ryzyka operacyjnego jest właśnie ryzyko informatyczne, definiowane przez Polską Normę jako: możliwość, że konkretne zagrożenie wykorzysta konkretną podatność systemu przetwarzania danych" [PN-I-02000:2002]. Natomiast zarządzanie ryzykiem informatycznym definiowane jest jako „proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, z zachowaniem akceptowalnego poziomu kosztów" [PN-ISO/IEC 17799].

Ryzyko informatyczne we współczesnej bankowości powinno podlegać interdyscyplinarnej segmentacji obszarowej ukierunkowanej na identyfikację odmiennych atrybutów ryzyka postrzeganego i analizowanego w różnych perspektywach, do których zaliczyć należy przede wszystkim (rys. 2):

- *perspektywę techniczną*, związaną z wykorzystywanym sprzętem i oprogramowaniem oraz jego konfiguracją, problemami zastosowań współczesnych metod kryptograficznych, technicznymi aspektami zarządzania dostępem do zasobów systemowych, a także zagadnieniami technicznej integracji systemów w procesach konsolidacyjnych,
- *perspektywę funkcjonalną*, w ramach której systemy informatyczne stosowane w instytucji bankowej można podzielić według ich funkcji na *core-banking*, systemy wspomagające zarządzanie (finanse, logistyka, kadry i płace, CRM itp.) oraz systemy bankowości elektronicznej,
- *perspektywę systemową*, oddzielającą systemy wykorzystywane tylko przez pracowników banku od systemów bankowości elektronicznej, do których dostęp mają także klienci banków,



Rys. 2. Obszary ryzyka informatycznego w ramach różnych perspektyw

Źródło: opracowanie własne.

- *perspektywę organizacyjną*, podkreślającą konieczność zarządzania ryzykiem także w obszarach pozatechnicznych, dotyczących czynnika ludzkiego, aspektów prawnych, strukturalnych i organizacyjnych, wdrożeniowych i konsolidacyjnych.

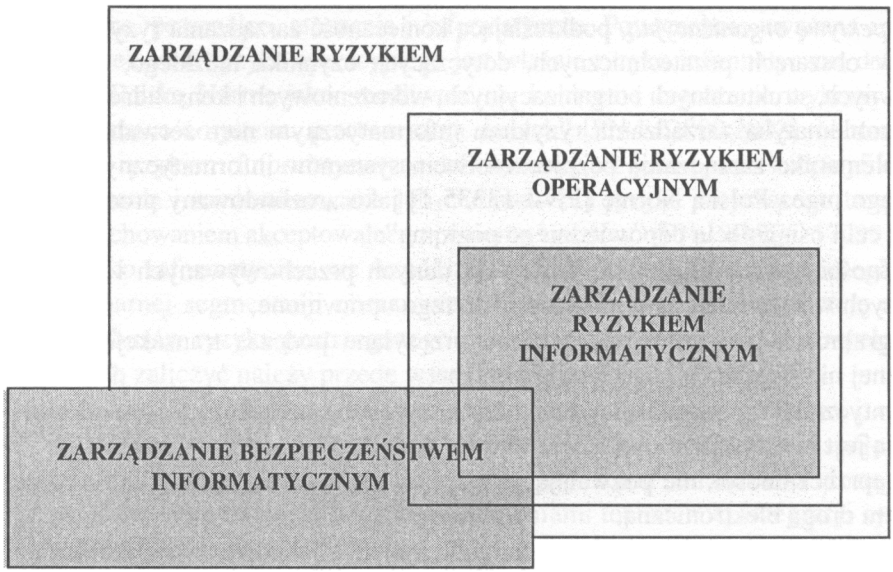
Z problematyką zarządzania ryzykiem informatycznym nierozerwalnie wiąże się problematyka zarządzania bezpieczeństwem systemów informatycznych, definiowanego przez Polską Normę [PN-I-13335-1] jako „rozbudowany proces stosowany w celu osiągnięcia odpowiedniego poziomu":

- poufności, gwarantującej, że dostęp do danych przechowywanych i przetwarzanych w systemie mają tylko osoby do tego uprawnione,
- integralności, gwarantującej, że dane przesyłane podczas transakcji elektronicznej nie są przez nikogo modyfikowane,
- autentyczności, pozwalającej stwierdzić, czy osoba podpisująca się pod transakcją jest rzeczywiście osobą, za którą się podaje,
- niezaprzeczalności, nie pozwalającej wyprzeć się nadania bądź odbioru komunikatu drogą elektroniczną,
- dostępności, gwarantującej stały dostęp do systemu bankowości elektronicznej,
- niezawodności, gwarantującej, że system działa w sposób, jakiego się od niego oczekuje.

Zarządzanie bezpieczeństwem jest procesem o charakterze cyklicznym. Z jednej strony można postrzegać go jako zbiór systematycznie realizowanych zadań, takich jak (zob. np. [Wawrzyniak 2002]):

- określenie potrzeb banku w zakresie ochrony danych,
- stworzenie polityki bezpieczeństwa (wybór modelu bezpieczeństwa, stworzenie Dokumentu zasad bezpieczeństwa),
- analiza ryzyka (identyfikacja i klasyfikacja aktywów systemu informatycznego, identyfikacja zagrożeń systemu, określanie podatności systemu na zagrożenia, ocena ryzyka, przedstawienie wyników analizy),
- wdrażanie systemu zabezpieczeń (wybór konkretnych rozwiązań, instalacja sprzętu i oprogramowania, szkolenia użytkowników systemu, zmiany organizacyjno-administracyjne),
- eksploatacja systemu zabezpieczeń (monitoring, ocena zastosowanych rozwiązań i zarządzanie zmianami, analiza i ocena poziomu bezpieczeństwa),
- z drugiej zaś jako metaobszar, w ramach którego identyfikuje się m.in. podobszary zarządzania ryzykiem, zmianami i czynnikiem ludzkim. Symboliczne zależności między obszarami zarządzania związanymi z ryzykiem informatycznym przedstawiono na rys. 3.

Aspektem istotnym dla problematyki zarządzania ryzykiem informatycznym jest identyfikacja zagrożeń bankowych systemów informatycznych. W najogólniejszym ujęciu zagrożenia te można podzielić, stosując podejście analogiczne do przestawionego wcześniej, bazujące na identyfikacji obszarów analizy problemu (rys. 2). Co więcej, obszary zdefiniowane w ten sposób charakteryzuje wielopłaszczyznowa



Rys. 3. Współistnienie obszarów zarządzania związanych z bezpieczeństwem informatycznym w instytucji bankowej

Źródło: opracowania własne.

przemienność. Na przykład, w ramach zagrożeń związanych z systemami bankowości elektronicznej można mówić o zagrożeniach w obszarach banku i klienta, w obszarach technicznym, kryptograficznym, dostępu itd. Świadectwem złożoności omawianej problematyki niech będzie lista najpoważniejszych zagrożeń związanych z wykorzystywaniem systemów bankowości elektronicznej w podziale na zagrożenia serwera, klienta oraz wspólne (zob. np. [Gospodarowicz 2005, s. 86 i nast.]).

Bezpieczeństwo klienta obejmuje ogół zagadnień związanych z wykorzystywaniem sprzętu i oprogramowania w celu komunikacji z bankiem internetowym. Do najpoważniejszych zagrożeń w tej grupie można więc zaliczyć:

- zagrożenia kompromitacji parametrów dostępu do systemu (identyfikator, hasło, lista haseł jednorazowych, PIN do tokena), będące następstwem łamania brutalnego, podsłuchu w sieci lokalnej, podsłuchu elektromagnetycznego, zastosowania oprogramowania szpiegującego lub metod typu *social-engineering*,
- manipulacje sprzętem i oprogramowaniem, mające na celu zmiany ich funkcjonalności niewidoczne dla użytkownika,
- błędy w oprogramowaniu standardowym (przede wszystkim w przeglądarkach),
- błędy w oprogramowaniu klienta (niestandardowym),
- niewłaściwe wykorzystanie technologii ActiveX,
- skrypty i aplety implementowane na stronach www,
- wirusy.

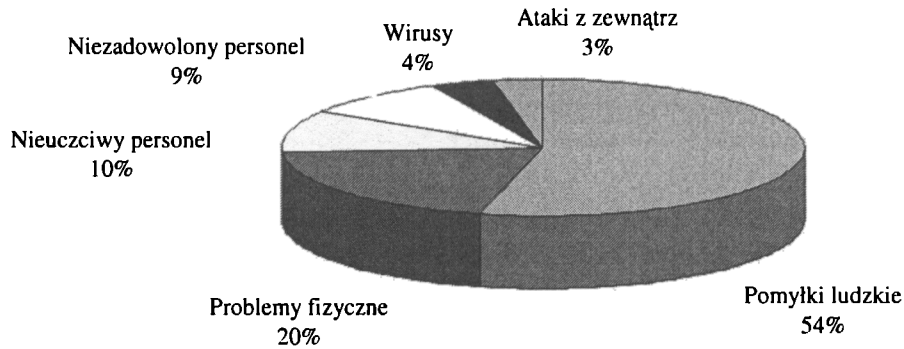
Zagrożeniami wspólnymi, związanymi z przesyłaniem danych sieciami komputerowymi, są:

- *sniffing*, czyli podsłuchiwanie, dzięki któremu można wejść w posiadanie danych przesyłanych sieciami,
- *spoofing*, polegający na podszywaniu się pod inny komputer w sieci, czyli na wysłaniu sfałszowanych pakietów do danej maszyny, aż do przejęcia całej sesji użytkownika z daną maszyną włącznie (*session hijacking*),
- *network snooping*, czyli wstępne rozpoznawanie parametrów sieci, zwłaszcza pod kątem stosowanych narzędzi bezpieczeństwa,
- zagrożenia związane z atakami typu *man-in-the-middle*,
- zagrożenia DNS (*domain name system*), w szczególności związane z podatnością usługi na ataki typu *denial of service*,
- zagrożenia usług SMTP, MIME, POP, WWW i innych,
- sabotaż komputerowy i cyberterroryzm.

Do zagrożeń serwera należą:

- *DOS* (*denial of service*), czyli atak, w którym jeden użytkownik zajmuje tyle dzielonych zasobów systemu, że następny użytkownik nie może już z nich skorzystać,
- wykorzystywanie specyficznych programów, umożliwiających ingerencję w systemy informatyczne, takich jak:
  - *bakterie* (*bacteria*), tj. programy, których jedynym przeznaczeniem jest powielanie się w celu zniszczenia systemu przez doprowadzenie do jego zablokowania,
  - *robaki* (*worms*), tj. programy przenoszące się z systemu na system w sieci, czasami pozostawiające po sobie bakterie lub wirusy,
  - *konie trojańskie* (*Trojan horses*), tj. programy, które udając, że wykonują bezpieczne operacje, w rzeczywistości wykonują działania mające na celu naruszenie bezpieczeństwa systemu. Najbardziej popularnym typem konia trojańskiego jest program kradnący hasło, który udaje normalną sekwencję rozpoczynania sesji, w rzeczywistości zaś zapisuje hasło wprowadzane przez użytkownika, a potem znika,
  - *bomby logiczne*, ukryte, nieudokumentowane fragmenty programów uruchamiane w określonym czasie bądź w następstwie określonego zdarzenia,
- uzyskiwanie dostępu do systemów poprzez *furtki* (*trap doors*), nieudokumentowane wejścia do legalnych programów, pozwalające zorientowanemu użytkownikowi omijać zabezpieczenia,
- ataki na bazy danych,
- wszystkie inne zagrożenia związane z funkcjonowaniem serwerów WWW,
- nielojalność i nieuczciwość pracowników banku,
- błędy i przeoczenia personelu obsługującego system,
- zagrożenia losowe, środowiskowe, czyli powodzie, pożary, wyładowania atmosferyczne, awarie zasilania, brud, kurz itd.,
- sabotaż komputerowy i cyberterroryzm.

Symbolicznym przedstawieniem problematyki zagrożeń systemów informatycznych w bankowości może też być statystyka częstości występowania zdarzeń związanych z poszczególnymi grupami zagrożeń systemów bankowych, sporządzona na podstawie badań ankietowych. Statystyka ta pokazuje, jak znaczący udział (w ujęciu ilościowym) we wszystkich sytuacjach naruszających bezpieczeństwo systemu mają te związane z działalnością samych pracowników banków, wyszczególnione w ostatniej części powyższego zestawienia (rys. 4).



Rys. 4. Zagrożenia bezpieczeństwa systemów informatycznych w bankowości

Źródło: [*Bezpieczeństwo*... 2003].

Ryzyko informatyczne jest takim rodzajem ryzyka bankowego, którego istnienie będzie z pewnością miało coraz większy wpływ na funkcjonowanie instytucji bankowych. Bardzo istotnym elementem, nie rozpoznanym jeszcze kompleksowo, wpływającym na to ryzyko, będzie niewątpliwie popularyzacja rozwiązań opartych na kwalifikowanym podpisie elektronicznym, zgodnym z ustawą. Czy implementacja regulacji ustawy przyniesie nie znane jeszcze zagrożenia? Na pewno tak, niemniej ważne jest, aby nie przesłoniły one korzyści wynikających z upowszechnienia technologii podpisu elektronicznego w bankowości.

Literatura

Bankowość elektroniczna, red. A. Gospodarowicz, PWE, Warszawa 2005.

Bezpieczeństwo systemów informatycznych w bankach w Polsce, red. J. Grzywacz, Oficyna Wydawnicza SGH, Warszawa 2003.

Operational Risk, Basel Committee on Banking Supervision 2001, http://www.bis.org/publ/bcbsca07.pdf.

Operational Risk Management, Basel Committee on Banking Supervision 1998, http://www.bis.org/publ/bcbs42.pdf.

Polska norma PN-I-02000:2002.
Polska norma PN-ISO/IEC 17799.
Rekomendacja_D, Komisja Nadzoru Bankowego 2002, http://www.nbp.pl/Publikacje /nadzor_ bankowy/pdf/rekomendacja_d.pdf.
Rekomendacja_M, Komisja Nadzoru Bankowego 2004, http://www.nbp.pl/Publikacje /nadzor_bankowy/pdf/rekomendacja_m.pdf.
Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, 2003, http://www.bis.org/publ/bcbs98.pdf.
Sound Practices for the Management and Supervision of Operational Risk, Basel Committee on Banking Supervision, 2003, http://www.bis.org/publ/bcbs96.pdf.
Wawrzyniak D., *Zarządzanie bezpieczeństwem systemów informatycznych w bankowości*, Wydawnictwo Zarządzanie i Finanse, Warszawa 2002.

INFORMATION RISK MANAGEMENT IN BANKING

Summary

The paper presents chosen aspects of information risk in banking. General ideas concerning the problem were described using the Basel Committee documents as well as NBP recommendations. The electronic banking security threats were presented as the crucial factors concerning information risk management. In addition the paper points to the role of non-technical aspects of risk management and information security management.