Ludosław Drelichowski, Hubert Zarzycki
Uniwersytet Technologiczno-Przyrodniczy w Bydgoszczy

Analiza skutków złożoności systemów informatycznych w banku spółdzielczym dla sprawnej obsługi klienta

Wstęp

Współczesne organizacje sektora finansowego w coraz większym stopniu uzależnione są od sprawnego funkcjonowania systemów informatycznych. Zachodzące procesy konsolidacji banków spółdzielczych powodują, że sieci komputerowe i stosowane systemy operacyjne ulegają coraz większej komplikacji. Dotyczy to również oprogramowania użytkowego niezbędnego do obsługi bankowości internetowej, home-bankingu czy zdalnego przetwarzania realizowanego w filiach centrali banku, komplikujące złożoność stosowanych technologii informacyjnych.

Niezbędne do wdrożenia w takiej strukturze organizacyjnej rozwiązania sieci komputerowych, systemów operacyjnych oraz systemów zdalnej interaktywnej obsługi klienta w małym banku złożonością rozwiązań systemowych nieznacznie tylko ustępują rozwiązaniom stosowanym w dużych bankach. Tym, co w zasadniczy sposób różnicuje sytuację tych dwu grup podmiotów, jest skala możliwości ponoszenia nakładów finansowych związanych z zastosowaniem technologii informacyjnych. Dotyczy to również możliwych do sfinansowania nakładów osobowych związanych z obsługą technologiczną i software'ową realizowanych w banku procesach informacyjnych. Możliwość zastosowania rozwiązań outsourcingowych również limitowana jest poziomem środków finansowych w stosunku do skali i złożoności zadań serwisowych. Należy sądzić, że wymienione wyżej uwarunkowania stanowiły jedną z przyczyn powoływania grup banków spółdzielczych, których zadaniem była współpraca w finansowaniu i rozwoju zastosowań opracowywanych w ramach poszczególnych grup bankowych systemów informatycznych. Jest to zadanie tym trudniejsze, że dynamika rozwoju produktów bankowych determinowana jest najczęściej przez odpowiednie standardy systemów informatycznych, równie ważnych z punktu widzenia sprawnej i merytorycznie poprawnej obsługi klienta. Coraz większa złożoność systemów informatycznych sprawia, że konieczne jest zastosowanie usługi ze-

wnętrznej – audytu informatycznego, polegającego na ocenie wdrożonych rozwiązań [Hysa 2007].

Celem artykułu jest przedstawienie złożoności stosowanych rozwiązań technicznych i programowych w przykładowym banku spółdzielczym, w celu oceny efektywności i bezpieczeństwa stosowanych rozwiązań informatycznych, które to problemy podejmowano wcześniej w tym sektorze [Drelichowski, Kamińska 2002]. Efektywne zarządzanie zasobami informatycznymi oparte jest na wiedzy o tym, jaki sprzęt komputerowy oraz jakie systemy operacyjne i aplikacje wchodzą w ich skład. Zwykle wiedza ta jest rozproszona pomiędzy poszczególne osoby korzystające z tych zasobów lub brak jej w ogóle. Taka sytuacja niekorzystnie wpływa na politykę organizacji dotyczącą zakupów sprzętu i oprogramowania komputerowego oraz na administrację tymi zasobami.

Jednym ze środków, które umożliwia uzyskanie szerszej informacji o posiadanych zasobach sprzętowych i zainstalowanym oprogramowaniu jest przeprowadzenie audytu informatycznego [Molski, Łecheta 2006]. W jego ramach można wyróżnić:

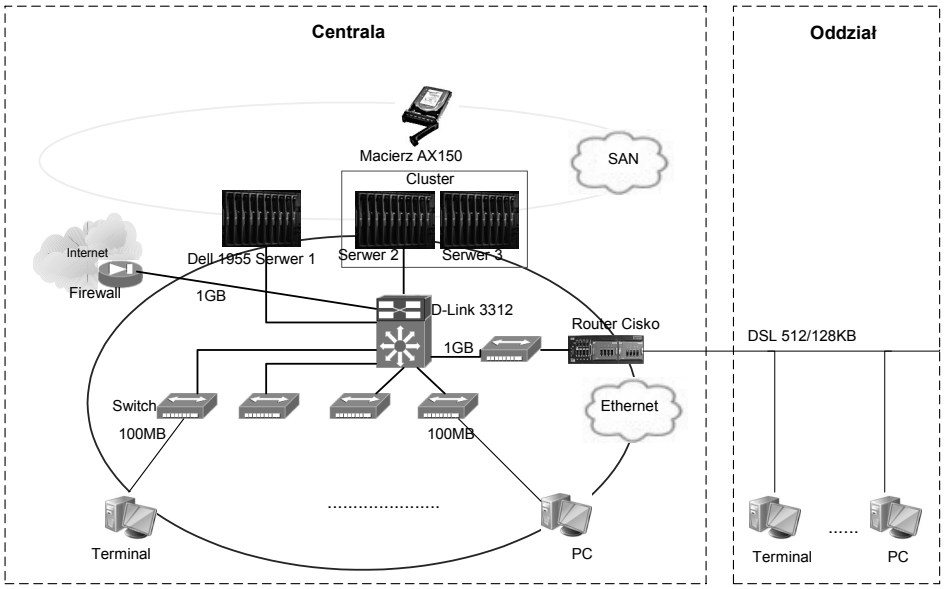
- audyt sprzętu,
- audyt oprogramowania,
- kontrolę nad systemami informatycznymi w organizacji,
- audyt legalności oprogramowania.

Ze względu na dynamikę rozwoju informatyki i wynikające z tego zmiany posiadania stanu zasobów firmy audyt informatyczny powinien być przeprowadzany co pewien okres, zależny od skali realizowanych zmian.

Audyt informatyczny można przeprowadzić we własnym zakresie lub zlecić wykonanie tego typu usługi firmie konsultingowej z zewnątrz [Forystek 2005]. Oba rozwiązania mają swoje zalety i wady, jednak fachowcy z zewnątrz mają tę przewagę, że posiadają odpowiednie narzędzia i doświadczenie potrzebne do wykonania takiego zadania. Ponadto wykonana przez nich ocena będzie niezależna i obiektywna. Dalsze części tego opracowania korzystają z wyników badań zamieszczonych w raporcie z audytu [Drelichowski i in. 2010] przeprowadzonego w jednym z banków spółdzielczych w województwie kujawsko-pomorskim.

Zasoby sprzętowe niezbędne do technologicznie wymaganego poziomu złożoności systemów informatycznych

Podstawę sprzętową systemów w badanym banku spółdzielczym stanowią serwery Dell PowerEdge 1955 podłączone do sieci SAN, do której również jest podłączona macierz AX150 (rys. 1). Macierz udostępnia zasoby dyskowe ser-



Rysunek 1
Uproszczony schemat infrastruktury banku
Źródło: Opracowanie własne na podstawie informacji zawartej na portalu internetowym organizacji.

werom Dell 1955. Serwery mają po 2 dyski lokalne skonfigurowane w RAID1. Sprzęt używany przez pracowników to stacje robocze z winXP, terminale z cienkim klientem i terminale na systemie LTSP. Przykłady konfiguracji sprzętowej można znaleźć w rozdziale zawierającym inwentaryzację sprzętu.

Na trzech serwerach Dell 1955 zostało zdefiniowane środowisko sieciowe. Serwery Blade 1955 posiadają po 2 karty ethernetowe. Obydwie karty sieciowe są podłączone do przełączników w obudowie bladów. W obecnej konfiguracji ruch jest rozkładany na obydwie karty, a w razie awarii jednego z przełączników ethernetowych komunikacja będzie odbywała się drugim. Zapewni to odporność na awarie fizycznych przełączników ethernetowych umieszczonych na obudowie bladów. Cała komunikacja z serwerami odbywa się przez 1 GB przełącznik D-link 3312. Większości sprzętu pracowników do komunikacji sieciowej używa połączeń o przepustowości 100 MB.

Do jednostek organizacyjnych banku można zaliczyć centralę, 4 oddziały i 2 filie. Centrala komunikuje się w jednakowy sposób ze wszystkimi oddziałami i filiami.

Na dwóch serwerach Dell 1955 został zainstalowany Vmware ESX Infrastruktury 3. Na serwerze trzecim został zainstalowany Vmware ESX Serwer 3i

i na maszynie wirtualnej Windows 2003 server, Virtual Center, SQL 2005 Workgroup edition oraz IT Assistant.

Obydwa serwery ESX zostały połączone w klaster z funkcjonalnością HA, DRS i Vmotion. High Availability umożliwia w razie awarii automatyczne uruchomienie maszyn na drugim serwerze. ESX.DRS zapewnia równomierne rozłożenie obciążenia na obydwa nody klastra i umożliwia automatyczne przeniesienie uruchomionych maszyn wirtualnych na innego noda w celu wyrównania obciążenia. Vmotion umożliwia przełączenie uruchomionej maszyny wirtualnej na inny serwer ESX. Na dwóch serwera są zainstalowane na maszynach wirtualnych systemy operacyjne Windows 2003 serwer, SUSE Linux Enterprise Server 10, SUSE Linux Enterprise Server 9, Linux Debian, Windows XP PRO.

Charakterystyczne parametry serwerów (blade'ów) w analizowanym Banku Spółdzielczym:

serwer 1:
XEON 5110 1.6GHZ/4MB 1066FSB 1 szt.
8GB PAMIECI FB 667MHZ FBD (8X1GB DUAL RAM)
serwer 2 i 3:
XEON 5110 1.6GHZ/4MB 1066FSB 2 szt.
16GB PAMIECI FB 667MHZ FBD (4X4GB DUAL RAM)

Serwery banku spółdzielczego można rozbudowywać o kolejne elementy. Serwery Dell Poweredge oparte na technologii blade mają wiele różnych możliwości rozbudowy. Najbardziej efektywny dalszy wzrost wydajności sprzętowej serwerów może się dokonać przez powiększenie pamięci operacyjnej, dokupowanie nowych blade'ów czy też zakup dodatkowych pamięci masowych.

Bardziej szczegółowa analiza rozwiązań i wydajności systemu komunikacyjnego, sieci VPN i dedykowanego do tych zadań sprzętu w banku spółdzielczym nie jest omawiana w tym opracowaniu ze względu na ograniczenia jego objętości.

Oprogramowanie użytkowe stosowane w banku

Bankowy system transakcyjny

Aplikacja Novum umożliwia obsługę dowolnej struktury bankowej:

- pojedynczy Bank,
- bank wieloplacówkowy z pracą zdalną oddziałów, filii i punktów kasowych przez łącze telekomunikacyjne,

- bank wieloplacówkowy z konsolidacją bilansu samodzielnych placówek bankowych,
- bank wieloplacówkowy z mieszaną infrastrukturą.
- System Novum-Bank pozwala stosować następujące metody obsługi klienta:
- handlowa – pozwalająca na obsługę klienta w zakresie wszystkich produktów oferowanych przez bank w jednym „okienku" – w jednej opcji programu,
- produktowa – pozwala na obsługę wg podziału produktowego, np. kredyty jedno „okienko", depozyty drugie itd.

Na jakość obsługi wpływa sposób komunikacji z klientem. System Novum-Bank umożliwia stosowanie:

- definiowanych dokumentów Banku, takich jak umowy kredytowe, formularze, informacje z automatycznym pobraniem danych z bazy banku,
- gotowych dokumentów jak np. różne typy wyciągów z rachunku (wysyłane pocztą e-mail, nadruk na gotowym formularzu),
- komunikację przez elektroniczne kanały dostępu: bankomat, home-banking, bankofon, SMS i Internet,

Dodatkowe cechy systemu Novum:

- może wykorzystywać architekturę klient – serwer (BS używa wywołania przez zdalny pulpit, tryb skaningowy),
- wysoka wydajność, pozwalająca obsłużyć jednocześnie ponad 10 000 użytkowników,
- niskie koszty eksploatacji bazy danych (użyta baza Progress ma niższe koszty eksploatacji niż porównywalne rozwiązania innych producentów),
- ograniczone do minimum czynności administracyjne,
- technologia powszechnie stosowana w bankach, urzędach administracji państwowej i samorządowej, przemyśle, szkołach wyższych,
- najwyższy poziom bezpieczeństwa w zakresie poufności, jak i technologii pracy,
- przenośność na dowolne platformy sprzętowe i systemy operacyjne (Windows, Unix, Linux).

Aplikacja do analizy kredytów

Aplikacja do analizy kredytów to kompleksowe rozwiązanie informatyczne wspierające departamenty kredytowe w ocenie wiarygodności kredytowej zarówno dla osób fizycznych, jak i szeroko rozumianych podmiotów gospodarczych. Analizator kredytowy to również narzędzie usprawniające procesy oceny i zarządzania wnioskami kredytowymi w Banku.

System oparty jest na wspólnej bazie danych (MS SQL Server), która pozwala analizować wszelkie występujące w banku transakcje kredytowe.

Pakiety biurowe Microsoft Office oraz Open Office

Pracownicy banku są niejednolicie wyposażenie w biurowe narzędzia informatyczne – pakiety MS Office i Open Office. Faktem jest większa uciążliwość korzystania z Open Office'a przez osoby będące operatorami systemu bankowego, którzy niezależnie od dostępnego i zalecanego w eksploatacji Open Office preferują logowanie do MS Office. W przypadku możliwości korzystania ze stanowiska posiadającego uprawnienia zdalnego dostępu do MS Office pracownicy stwierdzają dużo bardziej wydajną pracę w tym standardzie w stosunku do zdalnego dostępu do Open Office.

W opinii kierowników oddziału i pracowników operacyjnych ponad 95% klientów oczekuje wymiany informacji w standardzie MS Office. Warto zaznaczyć że w procesie dwustronnej konwersji formularzy z MS Office do Open Office następuje uszkodzenie formatu dokumentów wymagające wykonania dodatkowych czynności edytorskich. Oznacza to, że stosowane w celu oszczędności kosztów licencji rozwiązania Open Office wpływają na pogorszenie wydajności pracy tej grupy pracowników przez wielokrotną konwersję przygotowywanych i uzgadnianych zdalnie z klientem wersji dokumentów tekstowych i tablic excelowych.

Pozostałe oprogramowanie

Serwer pocztowy, który jest zorganizowany w oparciu o dystrybucję SUSE Linux Enterprise Server i bazę danych MySQL, jest w opinii wielu ekspertów najtańszym i w praktyce najlepszym rozwiązaniem pocztowym dla średniej wielkości przedsiębiorstw. Zorganizowanie serwera pocztowego banku spółdzielczego opartego na tych technologiach jest rozwiązaniem dopasowanym do skali i możliwości organizacji.

Dalsze zakupy oprogramowania użytkowego dyktowane są potrzebami dotyczącymi zapewnienia obsługi klienta – najczęściej są to rozwiązania posiadane wcześniej i rozwijane w poszczególnych bankach oraz zakupy dokonywane w ramach zrzeszeń banków spółdzielczych, związane z rozwojem oprogramowania koordynowanego w ramach grup bankowych. Wykorzystywane aktualnie

oprogramowanie w badanym banku spółdzielczym będzie wymagało modernizacji zgodnej z priorytetami wyznaczonymi w ramach grupy bankowej.

Kontrola nad systemami informatycznymi w organizacji

Polityka bezpieczeństwa oraz prawa dostępu pracowników

Microsoft w Windows 2003 Server położył szczególny nacisk na bezpieczeństwo. Wysoki stopień bezpieczeństwa został osiągnięty na wiele sposobów. Oprócz zmian w samej konstrukcji systemu przebudowano wiele składników w Windows. Zmieniony został również domyślny poziom bezpieczeństwa, ustawiany w czasie instalowania systemu operacyjnego. W Windows 2003 instalowane są tylko te składniki systemu, które są potrzebne do realizacji odpowiednich ról.

Administrator musi podjąć decyzję udostępnienia określonej usługi czy zezwolenia na dostęp użytkownikom do danego serwera. Przykładowo, domyślna instalacja serwera nie wgrywa Internet Information Server (IIS). Aby wgrać IIS, trzeba dodać rolę serwera aplikacyjnego, jednak nawet to nie uruchomi potencjalnie ryzykownych elementów. Aby np. możliwe było włączenie usługi indeksowania, musi zostać jawnie uruchomione odpowiednie rozszerzenie serwera IIS. Można to wszystko skonfigurować również z poziomu kreatora ról serwera. W Windows 2003 Server administrator powinien dokładnie określić, jakie usługi mają działać na serwerze.

Innym przykładem jest np. udostępnianie folderów. W Windows 2003 Server, jeżeli tworzony jest dzielony zasób sieciowy, to domyślnie grupa „wszyscy" może tylko czytać z tego zasobu.

Na bezpieczeństwo w Windows 2003 Server składa się kilka elementów – różne sposoby identyfikacji i autoryzacji użytkownika, listy dostępu i praw, a także polisy i inne mechanizmy pozwalające tworzyć spójną politykę bezpieczeństwa działania serwera.

Autoryzacja jest procesem weryfikacji obiektu, sprawdzeniem, czy rzeczywiście jest tym, za który się podaje. Logowanie się użytkownika do systemu przez podanie swojego identyfikatora oraz hasła jest najpowszechniejszym przykładem autoryzacji. Windows 2003 Server obsługuje także inne rodzaje autoryzacji (np. smart card).

W Windows 2003 Server dostępnych jest wiele różnych protokołów autoryzacyjnych. W zależności od zapotrzebowania można użyć jednej z opisanych

poniżej technik autoryzacji. Część z nich przeznaczona jest dla aplikacji WWW i służy ochronie poufności informacji umieszczanych na stronach internetowych lub intranetowych. Kolejne techniki służą do logowania się do Windows 2003 i np. pozwalają odczytywać zasoby Active Directory.

Prawa dostępu w Windows 2003 Server oparte są na tzw. listach DACL. Są to listy, w których każdy użytkownik lub grupa użytkowników ma przyznane ściśle określone prawa odnośnie obiektów występujących w systemie. Każdy aspekt działania Windows 2003 Server oparty jest na dostępie typu ACL (DACL).

Administrator może ustalać prawa dostępu do poszczególnych usług, drukarek, plików, folderów oraz kluczy rejestru za pomocą narzędzi systemowych. Po konfiguracji deskryptorów bezpieczeństwa w obiektach (np. Active Directory) grupy użytkowników uzyskują dostęp do podzbioru wszystkich praw i informacji.

DACL pozwala także na szczegółowe badanie operacji wykonywanych przez użytkownika. Można sprawdzić, kiedy użytkownik odwoływał się on do danego elementu lub też uzyskać informację, gdy ktoś próbuje uzyskać dostęp do obiektu, do którego nie uzyskał praw.

Do kluczowych pojęć związanych z listą kontroli dostępu DACL należą prawa dostępu. Prawa definiują, jakie operacje dany użytkownik (a raczej element o danym numerze SID) może wykonać na określonym obiekcie. Prawa mogą być przypisane m.in. do następujących obiektów:

- użytkowników/grup danej domeny,
- użytkowników/grup zdefiniowanych lokalnie na danym komputerze,
- użytkowników czy grup należących do innej domeny, ale połączonej relacją zaufania z administrowaną domeną,
- komputerów i innych dedykowanych obiektów występujących w Active Directory.

Zalecane jest tworzenie praw dla grup, a nie do poszczególnych użytkowników. Pełna lista możliwych rodzajów praw obejmuje kilkadziesiąt pozycji, w zależności od chronionego obiektu (np. inne będą dotyczyć pliku, a inne drukarki). Można jednak wyodrębnić cztery główne rodzaje praw:

- odczytu,
- modyfikacji,
- usunięcia obiektu,
- zmiany właściciela.

Należy pamiętać, że prawa zabraniające dostępu mają wyższy priorytet nad prawami udostępniającymi. Tak więc, jeżeli użytkownik należy do grupy A i B, przy czym grupa A ma prawa zapisu do określonego pliku, a grupa B nie może nadpisywać tego pliku, to wówczas użytkownik nie będzie mógł nic zapisać w danym pliku.

Obiekty kontrolowane przez Windows 2003 Server mają swoich właścicieli. Właścicielem domyślnie jest użytkownik, który stworzył ten obiekt. Bez względu na uprawnienia, właściciel zawsze może modyfikować prawa opisane w DACL dla stworzonego przez siebie obiektu. Może również zabrać sobie prawa do tego obiektu i je przywracać.

Dziedziczenia uprawnień jest jedną z ważniejszych zalet mechanizmu DACL. Można dzięki temu mechanizmowi ustalić, że wszystkie pliki lub podfoldery będą dziedziczyły uprawnienia z katalogu nadrzędnego. W Windows 2003 Server można precyzyjnie określić, które prawa mają być dziedziczone w obiektach potomnych.

Z przeanalizowanych przypadków i przykładów z literatury (np. w [Zalewski i in. 2009]) wynika, że prawa dostępu pracowników diagnozowanego banku spółdzielczego do katalogu wymiany, aplikacji i narzędzi systemowych są zorganizowane w prawidłowy sposób. Katalog wymiany jest dostępny do odczytu dla wszystkich, natomiast zapis jest możliwy jedynie we własnym podkatalogu pracownika. W podobny sposób jest zorganizowana kontrola dostępu do innych folderów. Do aplikacji w powszechnym użyciu typu Novum czy pakiet Office dostęp do zapisu, odczytu i wykonania mają wszyscy uprawnieni pracownicy. Z kolei dla aplikacji przeznaczonych dla określonych grup pracowników, np. managerów, analityków, prawa dotyczą tylko tej zadanej grupy pracowników.

Kontrola oparta na liście praw dostępu, praw dla grup i indywidualnych użytkowników jest poprawna. Prawa do odczytu, modyfikacji, usunięcia obiektu lub zmiany właściciela przydzielane są we właściwych przypadkach. Właścicielem obiektów jest administrator bądź uprawniona osoba (np. właściciel lokalnego zasobu). Uprawnienia są przydzielane do grup lub katalogów, co sprawia, że dziedziczenie uprawnień jest odpowiednie w obiektach potomnych. Prawa dostępu systemu Windows 2003 są skonfigurowane we właściwy sposób, aby zapewnić bezpieczeństwo systemu komputerowego.

Archiwizacja danych

Właściwa archiwizacja danych elektronicznych wiąże się z koniecznością spełnienia określonych wymagań prawnych. Regulują one zasady postępowania ze sferę bezpieczeństwa systemów, w których przechowywane są elektroniczne kopie danych.

Obowiązek tworzenia i zabezpieczania kopii zapasowych oraz ich przechowywania poza miejscem eksploatacji narzuca przedsiębiorcom ustawa o ochronie danych osobowych (art. 31). Z kolei ustawa z 29 września 1994 r. o rachunkowości podaje, że ochrona danych w trakcie prowadzenia ksiąg rachunkowych przy zastosowaniu komputera (księgi handlowe, dokumentacja inwen-

taryzacyjna, sprawozdania finansowe) powinna polegać na użyciu odpornych na zagrożenia nośników komputerowych. Wymagane jest również stosowanie środków ochrony zewnętrznej oraz systematyczne tworzenie rezerwowych kopii bezpieczeństwa danych zapisywanych na nośnikach danych [Pańkowska 2009, Winiarska 2008].

Kolejnym warunkiem, który należy spełnić, jest zapewnienie trwałości zapisu informacji systemu rachunkowości przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych (tzn. przez 5 lat).

Również rekomendacja Generalnego Inspektora Nadzoru Bankowego, dotycząca zarządzania ryzykiem towarzyszącym systemom informatycznym i telekomunikacyjnym używanym przez banki, stanowi: „Konieczne jest stosowanie kopii bezpieczeństwa (tzw. backup) i bieżącego dziennika zdarzeń (tzw. log), które w przypadku utraty danych powinny pozwolić na odtworzenie zasobów. Kompletne zapisy kopii zapasowych (backup) powinny być przechowywane oddzielnie, w odpowiednim oddaleniu od systemu informatycznego, dobrze zabezpieczone fizycznie i środowiskowo".

Podsumowanie

Zamieszczony w pracy przegląd struktury oraz funkcji realizowanych przez systemy użytkowe eksploatowane przez bank spółdzielczy składający się z 4 oddziałów i 2 filii uświadamia skalę złożoności rozwiązań systemowych eksploatowanych w tych organizacjach. Spełnienie odpowiednich wymagań bezpieczeństwa oraz dostatecznej sprawności obsługi klienta powoduje, że nakłady na sprzęt komputerowy, oprogramowanie podstawowe (systemy operacyjne, zarządzanie sieciami komputerowymi), licencje Systemów Zarządzania Bazami Danych i oprogramowanie biurowe oraz oprogramowanie użytkowe powodują wysokie koszty zakupu. Zapewnienie efektywnej eksploatacji tego niezwykle złożonego środowiska technologii informacyjnych wymaga zapewnienia profesjonalnego nadzoru, wiąże się też ze znacznym ryzykiem cyklicznego „zawieszania się" systemu operacyjnego, połączonego z koniecznością restartu i przerwą w jego pracy.

Najważniejsze wnioski i zalecenia przedstawione po przeprowadzeniu audytu IT w banku spółdzielczym obejmującego sprzęt i komunikację, oprogramowanie, legalność software'u, zabezpieczenia oraz politykę bezpieczeństwa są następujące:

1. Zabezpieczenia i prawa użytkowników oparte na Windows 2003 nie budzą zastrzeżeń, natomiast konieczne jest opracowanie szczegółowych instrukcji precyzujących całościową politykę bezpieczeństwa banku zgodną z ogólnie

przyjętymi standardami, co powinno być wykonywane przez specjalistyczne firmy dokonujące certyfikacji.

2. Spełnienie wymagań dotyczących zapewnienia poprawności z ustawowymi regulacjami księgowości dotyczącymi banków muszą być zapewnione przez dostawcę systemu transakcyjnego do obsługi banku oraz usługi wsparcia związane z eksploatacją tego systemu.

3. Kolejne działania telekomunikacyjne powinny uwzględniać dwa elementy związane z transferem informacji między oddziałami a centralą. Obydwa te elementy stanowią zagrożenia wpływające na ograniczenie wydolności systemu transmisji.

Sugeruje się wykonanie następujących działań:

1. Zwiększyć przepustowość łączy między siecią IP a systemem informatycznym w oddziale, co oznacza, że łącza ADSL 512 kb/s w dół sieci oraz 128 kb/s w górę sieci należy zamienić na łącza 2 Mb/s w dół sieci oraz 512 kb/s w górę sieci. Ze względu na zbliżony do symetrycznego charakter ruchu w oddziałach sugeruje się sprawdzenie możliwości dostarczenia w nich łączy symetrycznych.

2. Zwiększyć przepustowość symetrycznego łącza między centralą a siecią TP SA z 1 Mb/s w dół i w górę na łącze 4 Mb/s w dół i w górę.

Analiza ograniczeń wynikających z eksploatacji MS Windows 2003 uzasadnia przejście na MS Windows 2008, którego licencja w wersji 32- i 64-bitowej jest już dostępna w banku. Zaleca się zakup serwera (blade'a), na którym będzie można uruchomić testową wersję systemu Windows 2008. Przed zakupem dodatkowego serwera istnieje możliwość prowadzenia testów wdrożeniowych przez instalację systemu Windows 2008 tylko z wykorzystaniem oprogramowania VMware na już istniejącym sprzęcie.

Literatura

DRELICHOWSKI L., KAMIŃSKA K., Analiza zakresu zdalnej obsługi klientów w ramach technik informacyjnych stosowanych w lokalnym banku. Folia Oeconomica 157, Wyd. UŁ Łódź 2002. s. 371–385.

DRELICHOWSKI L., ZABŁUDOWSKI. A., ZARZYCKI H.: *Audyt Informatyczny w Banku Spółdzielczym*, na zlecenie Spółdzielcza Grupa Bankowa Bank Spółdzieczy w „X", Wydział Zarządzania i Wydział Telekomunikacji i Elektrotechniki UTP, Bydgoszcz 2010.

FORYSTEK M.: *Audyt informatyczny*, InfoAudit, Warszawa 2005.

HYSA B.: Audyt informatyczny jako narzędzie doskonalenia funkcjonowania organizacji, Systemy Wspomagania Organizacji, Katowice 2007.

MOLSKI M., ŁECHETA M.: *Przewodnik audytora systemów informatycznych*. Helion, Gliwice 2006.

PAŃKOWSKA M.: *Audyt informatyczny w jednostkach sektora finansów publicznych*, Polskie Towarzystwo Zarządzania Produkcją, Konferencja Komputerowo Zintegrowane Zarządzania, Zakopane 2009.
WINIARSKA K.: *Audyt wewnętrzny*, Difin, Warszawa 2008.
ZALEWSKI A., CEGIEŁA R., SACHA K.: *Modele i praktyka audytu informatycznego*, e-Informatyka.pl 2009.

Analysis of effects computer's complexity systems in the cooperative bank for the efficient service of the customer

Abstract

In this paper the range of bank products offered at Cooperative Banks acting in the structure of a few branches and division was presented. This requires applying the top complexity information technology. The purchasing of advanced equipped servers causes it in appropriate of memory in house and mass services providing supporting the accomplishment for the function of the customer are needed.

The technology of processing must provide the service of the customer in the headquarter of the bank and the remote system carried out as part of the Internet banking and home-banking.