Andrzej Koziara

Barbara Wróbel
Oddział Obsługi Informatycznej
Bibliotek Uniwersytetu Śląskiego

Koncepcja ochrony sieci i informacji w systemie biblioteczno-informacyjnym Uniwersytetu Śląskiego

Pojęcie ochrony sieci komputerowych doczekało się w prasie specjalistycznej ogromnej ilość artykułów. Artykuły te z reguły opisują przykłady, w których tak naprawdę użytkownikami wewnętrznej sieci komputerowej są tylko i wyłącznie pracownicy firmy, której opis dotyczy. Już sam ten fakt pokazuje nam, że tak naprawdę opracowań dotyczących instytucji otwartych, jakimi są biblioteki, jest bardzo mało. Równocześnie musimy zdawać sobie sprawę, że sama prosta ochrona sieci nie będzie dla nas satysfakcjonująca. Powinniśmy ją poszerzyć o ochronę informacji, która jest produkowana i gromadzona w naszej instytucji.

Artykuł ten został opracowany z dwóch przyczyn. Pierwszą jest zaprezentowanie metodyki prowadzenia analiz w specyficznych jednostkach, jakimi są biblioteki, a szczególnie biblioteki naukowe. Druga to zasygnalizowanie możliwości oprogramowania ISA (*Internet Security and Acceleration Server*) firmy Microsoft. Mimo całej nadmiernie demonstrowanej niechęci środowiska informatycznego do tej firmy, należy przyznać, że wiele jej produktów przygotowywanych w sposób bardzo kompleksowy potrafi zapewnić nam wysoki poziom bezpieczeństwa, a co za tym idzie wysoki komfort pracy.

Sam proces opracowania oraz wdrożenia koncepcji jest stosunkowo długi i żmudny. Nie można tutaj zastosować żadnych uproszczeń i uogólnień. Równocześnie niedopuszczalne jest zezwolenie służbom informatycznym na bezmyślny dyktat w myśl zasady "ciąć, ciąć, ciąć, bez przyczyn i umiaru wszystko, co popadnie".

Według naszej oceny, dla systemu informatyczno-bibliotecznego Uniwersytetu Śląskiego proces wdrożenia powinien zostać przeprowadzony w następujących etapach:

I. analiza struktury systemu biblioteczno-informacyjnego oraz zadań spełnianych przez jego elementy;
II. identyfikacja źródeł zagrożeń wraz z oceną ryzyka, jakie one niosą ze sobą;
III. analiza rzeczywistych potrzeb;
IV. przegląd rozwiązań możliwych do implementacji;
V. projekt implementacji wybranego systemu dostosowanego do potrzeb systemu bibliotecznego UŚ.

Ad. I Analiza struktury

1. Jednostki organizacyjne
    - Biblioteka Uniwersytetu Śląskiego z wydzielonymi specjalistycznymi działami do obsługi czytelników oraz działami zaplecza (komputery pracownicze oraz dostępne w czytelniach przeznaczone do wykonywania wszystkich operacji

bądź tylko do wydzielonych celów);
    - duże biblioteki specjalistyczne strukturą zbliżone do BUŚ - wydzielone osoby obciążone w mniejszym zakresie pracą z czytelnikiem. Komputery dla czytelników są "maszynami uniwersalnymi";
    - małe biblioteki specjalistyczne stanowiące jednostki uniwersalne przy jedno- lub kilkuosobowej obsadzie realizujące wszystkie funkcje "po trochę".
2. Lokalizacja jednostek
    - kampus główny - Katowice, ul. Bankowa;
    - rozrzucone jednostki w miastach: Katowice, Sosnowiec i Cieszyn - sześć lokalizacji;
    - pojedyncze jednostki w Chorzowie, Jastrzębiu i Rybniku.
3. Zadania Biblioteki Uniwersytetu Śląskiego
    - udostępnianie zasobów własnych wraz z całym cyklem przygotowania tych zasobów (zakup i opracowanie) poprzez wypożyczenie ich do domu oraz udostępnianie ich na miejscu w czytelniach;
    - udostępnianie elektronicznych i tradycyjnych źródeł informacji w czytelniach BUŚ (szczególnie w Czytelni Oddziału Informacji Naukowej);
    - prowadzenie technologiczne systemów informatycznych wspomagających działalność sieci biblioteczno-informacyjnej Uniwersytetu Śląskiego;
    - technologiczne wspomaganie sieciowego rozpowszechniania elektronicznych źródeł informacyjnych (system InfoWare CH/HD - IRIS XP) oraz zdalnego, kontrolowanego do nich dostępu (Onelog);
    - zapewnienie zaplecza sprzętowego i oprogramowania niezbędnego do prowadzenia szkoleń personelu i czytelników;
    - szkolenie personelu własnego i pracowników sieci bibliotek specjalistycznych w zakresie użytkowania zasobów elektronicznych oraz innych czynności niezbędnych w pracy biblioteki (opracowanie i aplikacje biurowe);
    - szkolenie czytelników w zakresie użytkowania elektronicznych źródeł informacji i innych systemów informacyjnych UŚ.
4. Zadania bibliotek specjalistycznych
    - udostępnianie zasobów własnych wraz z całym cyklem przygotowania (w szczególności wypożyczenia masowe dla studentów);
    - udostępnianie zasobów elektronicznych na wolnodostępnych stanowiskach komputerowych (w większości bibliotek specjalistycznych liczba komputerów jest zbyt mała, jak na potrzeby czytelników);
    - szkolenie pracowników i studentów w zakresie korzystania z elektronicznych źródeł informacji.
5. Użytkowany sprzęt
    - BUŚ - stanowiska komputerowe od najnowszych do Pentium 90 wykorzystywanych jako terminale graficzne do serwerów aplikacyjnych;
    - biblioteki specjalistyczne sieci - wyposażenie podobne jak w BUŚ.
6. Użytkowane sieci komputerowe
    - BUŚ - wydzielona fizycznie sieć komputerowa w ramach kampusu głównego UŚ. Mimo lokalizacji w budynku mieszczącego kilka jednostek organizacyjnych posiada własne przyłącze do głównego routera Uniwersytetu Śląskiego;
    - biblioteki specjalistyczne sieci - posiadają niewydzielone fizycznie sieci przyłączone bezpośrednio do sieci budynkowych. W zależności od ich lokalizacji mogą one stanowić również element struktury kablowej jednostek "obcych".

Ad. II Identyfikacja źródeł zagrożeń

1. Zagrożenia zależne od spełnianych statutowo zadań przez biblioteki naukowe
    - konieczność dostosowania stanowisk do spełnianych celów - brak możliwości blokowania wielu funkcji, zwykle wyłączanych przez administratorów;
    - dynamiczne zmiany wprowadzane przez dostawców informacji płatnej;
    - podatność stanowisk na oprogramowanie automatycznie instalujące się z sieci Internet.
2. Zagrożenia zależne od struktury organizacyjnej sieci bibliotek
    - brak wydzielonego systemu okablowania dla bibliotek specjalistycznych;
    - brak logicznego przydziału ról dla poszczególnych stanowisk komputerowych (brak personelu, miejsc i sprzętu);

- zła praca administratorów lokalnych sieci komputerowych oraz administratorów stacji roboczych.

3. Zagrożenia związane z celowym działaniem czytelników biblioteki, studentów w ramach zajęć w pracowniach i laboratoriach oraz intruzów z zewnątrz
   - instalowanie oprogramowania zbędnego oraz groźnego dla stabilności systemów operacyjnych stacji roboczych;
   - świadome i nieświadome instalowanie oprogramowania otwierającego dziury w systemach operacyjnych, umożliwiającego intruzom z zewnątrz przejęcie kontroli nad stacjami roboczymi;
   - świadome i nieświadome uruchamianie oprogramowania instalującego w systemach operacyjnych tzw. konie trojańskie;
   - świadome działania intruzów z zewnątrz próbujących wykorzystania istniejących luk w systemach operacyjnych, aby przejmować kontrolę nad stacjami roboczymi i przy ich użyciu dokonywać włamań do kolejnych systemów komputerowych.
4. Zagrożenia związane z działaniami (o nieznanym zakresie) innych użytkowników sieci komputerowych Uniwersytetu Śląskiego
   - wpływ zawirusowanych stacji roboczych spoza bibliotek na stacje robocze zainstalowane w bibliotekach;
   - celowe działania innych użytkowników mające wpływ na działanie sieci i stacji roboczych w bibliotekach specjalistycznych;
   - celowe działania dezintegrujące stacje robocze w bibliotekach specjalistycznych przez osoby z zewnątrz korzystające z komputerów naszej instytucji.

Ad. III Analiza rzeczywistych potrzeb

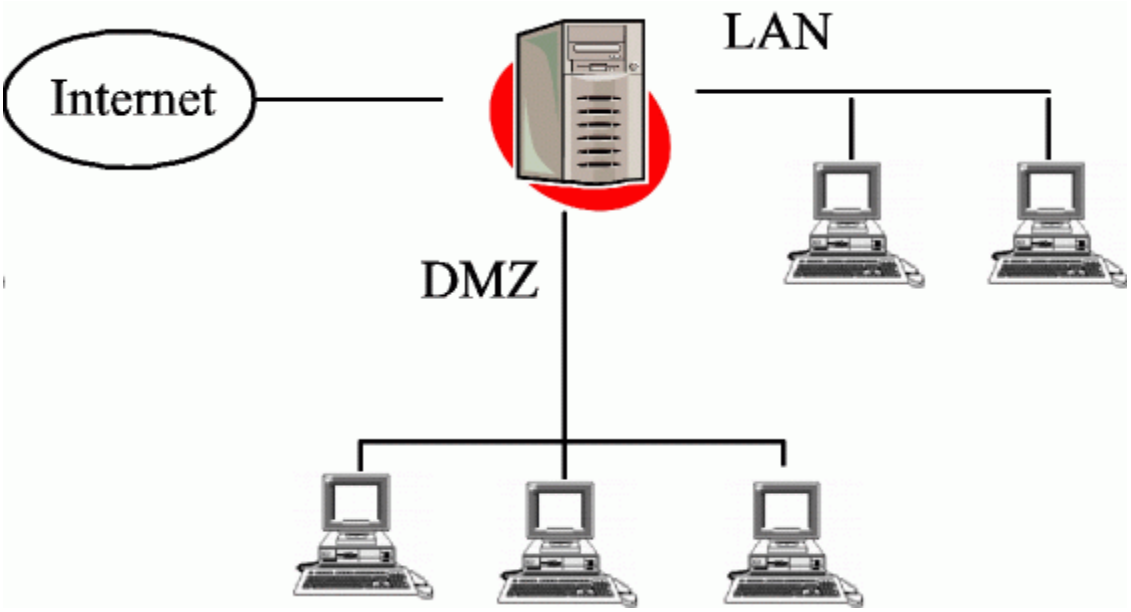
1. Potrzeby związane z ochroną systemów centralnych instalowanych na serwerach bazodanowych oraz aplikacyjnych
   - ochrona przed nieuprawnioną, celową ingerencją w system przez osoby niemające praw, tak do administrowania, jak i użytkowania serwerów;
   - ochrona przed oddziaływaniem niepożądanego oprogramowania umożliwiającego przejęcie kontroli nad serwerami;
   - ochrona przed utratą danych składowanych w katalogach osobistych użytkowników.
2. Potrzeby związane z ochroną stacji roboczych bibliotekarzy i innych pracowników bibliotek
   - ochrona przed niecelowymi, nieuprawnionymi działaniami użytkowników stacji roboczych;
   - ochrona przed nieuprawnioną, celową ingerencją w systemy przez osoby niemające praw (włamania i przejęcia kontroli);
   - ochrona przed oddziaływaniem niechcianego oprogramowania umożliwiającego przejęcie kontroli nad stacjami roboczymi, tak z komputerów w systemie informacyjno-bibliotecznym UŚ, jak i spoza jego obszaru;
   - ochrona przed utratą danych składowanych w katalogach osobistych użytkowników;
   - ochrona przed oddziaływaniem wirusów i innego oprogramowania instalującego się automatycznie z odwiedzanych witryn internetowych;
   - rozdzielenie pracowników na różne grupy robocze w zależności od spełnianych zadań - komputery przydzielone do tych grup są podłączane do innych fizycznych fragmentów sieci komputerowej.
3. Potrzeby związane z ochroną bądź ograniczaniem możliwości stacji roboczych przeznaczonych dla czytelników
   - ochrona przed instalowaniem oprogramowania przez użytkowników systemu;
   - ochrona przed zmianami konfiguracji stacji przez niesfornych czytelników;
   - ochrona przed wykorzystywaniem niedozwolonego oprogramowania;
   - racjonalne rozdzielenie czytelników na różne grupy robocze w zależności od charakterystycznych dla nich potrzeb - komputery przydzielone do tych grup są podłączane do innych fizycznych fragmentów sieci komputerowej.
4. Potrzeby związane z procedurami ochrony danych osobowych gromadzonych w bazach użytkowanych na terenie systemu biblioteczno-informacyjnego Uniwersytetu Śląskiego

- ograniczenie dostępu tylko dla wyznaczonych stacji roboczych z terenu całego UŚ;
- szyfrowanie przesyłanych danych.

Jak możemy zauważyć, zewidencjonowane powyżej zadania musza być realizowane wielotorowo i wymagają zaprojektowania całego systemu informatycznego, który będzie realizował te funkcje w sposób racjonalny oraz bardzo sprawny. Oczywiście jednym z elementów takiego systemu musi być bezpieczne i sprawne rozwiązanie zarządzające siecią. Musi ono być tak przygotowane, by w przyszłości istniała możliwość integracji bibliotek specjalistycznych łączących się bezpośrednio z centralą przez bezpiecznie szyfrowane kanały VPN (*Virtual Private Network*).

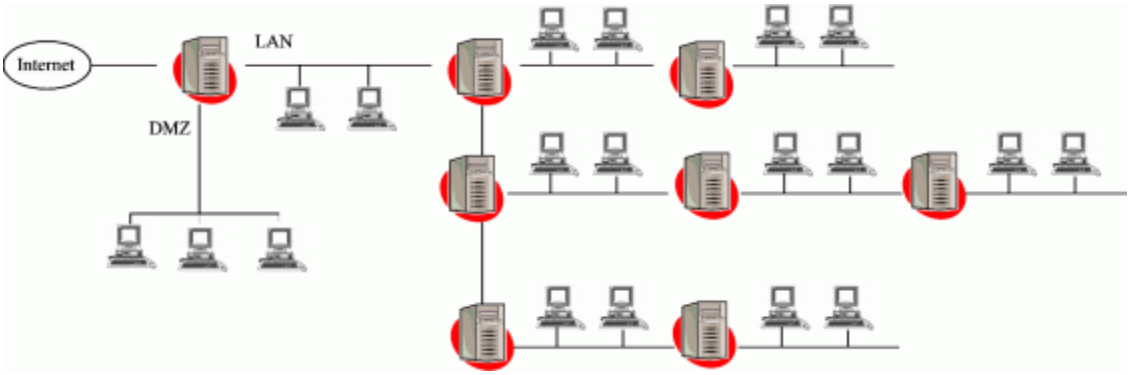
Ad. IV Przegląd rozwiązań możliwych do implementacji na terenie UŚ

1. Rozwiązanie klasyczne



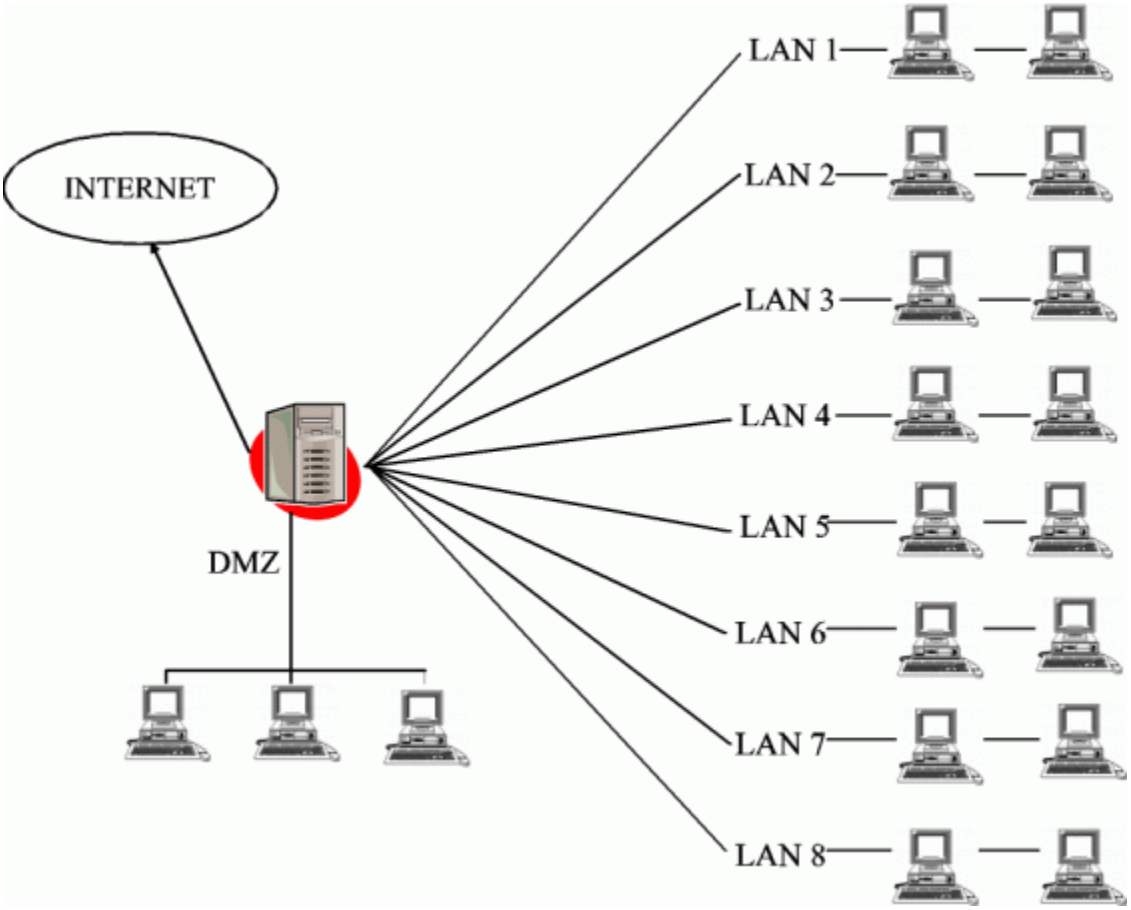
Jak widać, propozycja powyższa jest praktycznie niewystarczająca nawet w stosunku do części naszych potrzeb. Mogłaby spełnić tylko i wyłącznie jedno wymaganie - ograniczenie wykonane na jednym poziomie w zakresie dostępu do komputerów zainstalowanych w sieci wewnętrznej. Dla biblioteki naszej wielkości sieci wewnętrznych będzie kilka lub kilkanaście i w każdej takiej sieci muszą obowiązywać inne reguły i poziomy zabezpieczeń. Rozwiązanie to ma jeszcze jedną wadę, tzw. strefa zdemilitaryzowana (DMZ) jest tylko jedna i nie ma możliwości pogrupowania serwerów ze względu na funkcje, które one spełniają.

2. Rozwiązanie drabinkowe



Kolejnym pomysłem, który analizowaliśmy był tzw. układ drabinkowy. Charakteryzuje się on tym, że komputery są pogrupowane tak, by kolejne systemy firewall ograniczając uprawnienia, wprowadzały coraz wyższe poziomy zabezpieczeń. Po przeprowadzeniu dogłębnych studiów okazało się, że rozwiązanie to pomimo wysokich nakładów kosztów i pracy nie zapewni wszystkich cech bezpiecznej sieci.

3. Rozwiązanie gwiaździste



Podstawą naszego projektu były następujące założenia:

- system powinien być zaprojektowany tak, by aktualne potrzeby użytkowe sieci bibliotecznej decydowały o ilości sieci w części wewnętrznej (LAN);
- system powinien dawać możliwość deklarowania w sposób indywidualny uprawnień do łączności pomiędzy komputerami podłączonymi w rożnych gałęziach wewnętrznych (LAN1, LAN2, ...);
- system powinien zawierać oprogramowanie kontrolujące w warstwie aplikacyjnej dopuszczalność do współpracy komputerów zainstalowanych w różnych gałęziach wewnętrznych.

Ad. V. Projekt implementacji wybranego systemu do ochrony sieci komputerowych w systemie biblioteczno-informacyjnym Uniwersytetu Śląskiego

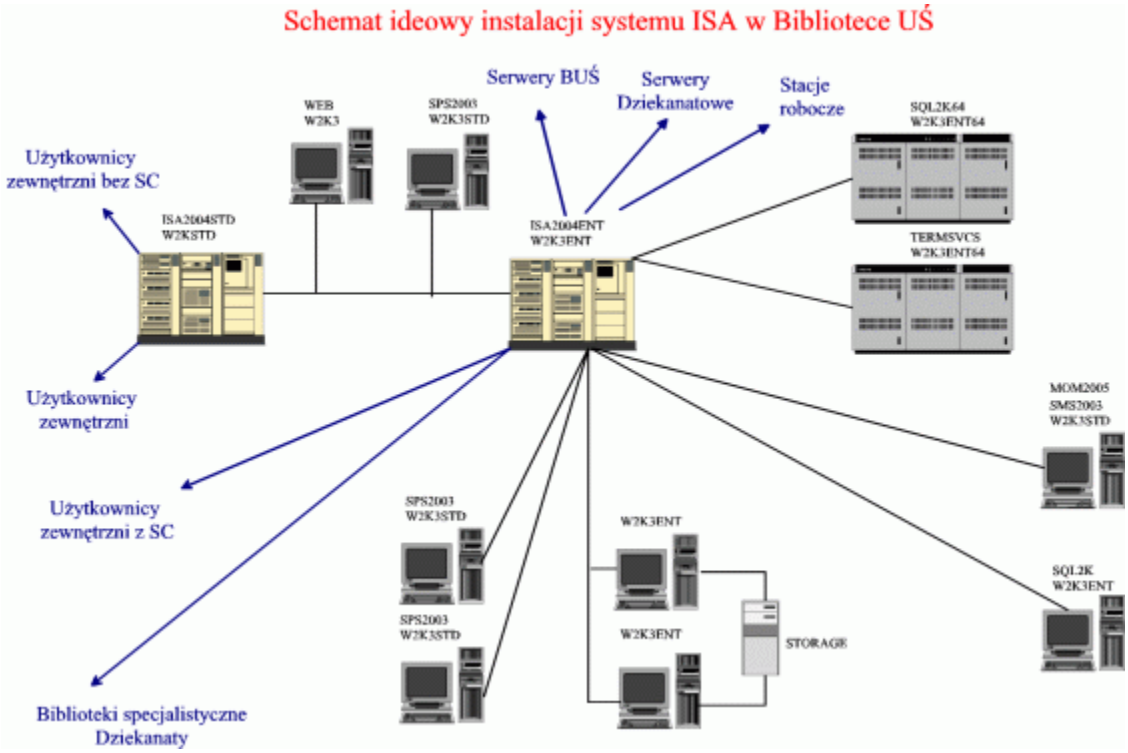
Podczas przygotowania projektu rozwoju systemów powyższe założenia uzupełniliśmy o kolejną ich grupę, związaną z porządkowaniem struktur organizacyjnych. Zawierają one:

- projekt optymalizacji wykorzystania licencji na oprogramowanie użytkowe poprzez jednolite i jednorazowe instalowanie ich na serwerach aplikacyjnych;
- projekt jednolitego składowania dokumentów produkowanych w systemie informacyjno-bibliotecznym Uniwersytetu Śląskiego poprzez jednolitą platformę

dostępową oraz składowanie ich w jednolitej bazie danych. Projekt zawiera również system wykonywania kopii zapasowych oraz system tzw. wersjonowania dokumentów. Umożliwi on również grupową, równoczesną pracę nad jednym dokumentem wielu użytkownikom systemu;

- projekt bezpiecznego połączenia bibliotek specjalistycznych z centralą w BUŚ. W projekcie tym uczestniczyć będą również komputery zainstalowane w dziekanatach (w systemie bibliotecznym UŚ oraz w systemie dziekanatowym UŚ przechowywane są dane osobowe podlegające ochronie zdefiniowanej wg identycznych przepisów prawa);
- projekt mechanizmu umożliwiającego automatyczne monitorowanie pracy wszystkich zainstalowanych serwerów;
- projekt mechanizmu automatyzującego aplikowanie poprawek do systemów operacyjnych stacji roboczych.

Najogólniej efekty naszych prac studialnych możemy przedstawić na schemacie opublikowanym poniżej.



Obecnie przystąpiliśmy do tworzenia środowiska testowego, które posłuży nam w przyszłości jako zalążek systemu roboczego (produkcyjnego). Liczymy na to, że wdrażając kolejne etapy projektu, doprowadzimy do znacznego uporządkowania systemów informatycznych i obniżenia kosztów oraz znacznego zwiększenia bezpieczeństwa użytkowników.

Koncepcja ochrony sieci i informacji w systemie biblioteczno-informacyjnym Uniwersytetu Śląskiego / Andrzej Koziara, Barbara Wróbel// W: Biuletyn EBIB [Dokument elektroniczny] / red. naczelny Bożena Bednarek-Michalska. - Nr 5/2005 (66) maj. - Czasopismo elektroniczne. - [Warszawa] : Stowarzyszenie Bibliotekarzy Polskich KWE, 2005. - Tryb dostępu: http://www.ebib.pl/2005/66/wrobel.php. - Tyt. z pierwszego ekranu. - ISSN 1507-7187