# SPOŁECZNA WYŻSZA SZKOŁA PRZEDSIĘBIORCZOŚCI I ZARZĄDZANIA W ŁODZI

KIERUNEK STUDIÓW: **INFORMATYKA**

Doniak Grzegorz
Numer albumu: ...27897....


# Dobór systemów i backupów dla danego przedsiębiorstwa.

Praca inżynierska napisana
w Instytucie Technologii Informatycznych
pod kierunkiem
...dr inż. Piotr Goetzen.....

**Łódź 2010**

# Spis treści

# 1. Wstęp

Realizacja bezpiecznego sposobu przesyłania informacji ich archiwizowania i backupu jest obecnie jednym z najważniejszych, jeżeli nie najważniejszym z wyzwań stojących przed globalną siecią. Rozpowszechnianie się elektronicznych usług całkowicie zmienia model światowego handlu. To wiedza i dostępność informacji decydują o pozycji na rynku, prestiżu, dochodach, zarówno jednostek jak i całych przedsiębiorstw. Wszystko to powoduje ciągły wzrost wartości danych, które im są cenniejsze, tym bardziej narażone na niebezpieczeństwa. Najwygodniej przyjąć założenie, iż wszystkie dane i informacje, zarówno te przesyłane jak i magazynowane, powinny być przez cały czas jak najlepiej chronione. Należy jednak pamiętać, że każdy zastosowany w tym celu środek bezpieczeństwa oznacza dodatkowe koszty. Przed podjęciem decyzji dotyczących czasu i nakładów, jakie będą przeznaczone na stworzenie odpowiednich zabezpieczeń, komercyjne firmy oceniają wartość samych informacji. To od niej zależy poziom i rodzaj środków, jakie będą przeznaczone na zapewnienie adekwatnego poziomu ochrony. Aby chronić informacje, nie trzeba jednak dysponować ogromnym budżetem.

## 1.1. Cel i zakres pracy

Celem niniejszej pracy jest przybliżenie tematyki backupu danych oraz projekt sieci komputerowej z wdrożeniem systemu serwerów backupowych.

## 1.2. Układ pracy

Praca składa się z dwóch głównych rozdziałów. Pierwszy z nich zawiera wprowadzenie do tematyki archiwizacji danych, przedstawia rodzaje backupów oraz jego strategie. W rozdziale tym zaprezentowano także rodzaje pamięci masowych przeznaczonych do archiwizacji danych, kładąc duży nacisk na powszechnie stosowane macierze RAID. W drugim rozdziale zaprezentowano projekt sieci dla firmy średniej wielkości uwzględniający potrzebę backupu danych.

## 2. Wprowadzenie do tematyki archiwizacji danych

Korzystanie z Internetu wiąże się z ryzykiem. Jedna z jego najdoskonalszych własności – wzajemny dostęp do siebie wszystkich połączonych komputerów – okazuje się jednocześnie jedną z największych wad. Każdy anonimowy użytkownik może żądać dostępu do usług oferowanych przez serwer. Większość tych żądań dotyczy tylko wyświetlenia określonej strony internetowej, jednak włączenie komputera do sieci umożliwia nawiązanie z nim również połączeń innego rodzaju. Założenie, iż jedynym dobrym rozwiązaniem jest przedsięwzięcie wszystkich dostępnych środków ostrożności, mających zapewnić komputerom pełne bezpieczeństwo (na przykład odłączenie ich od sieci lub wyłączenie) jest błędne. W celu udostępnienia pewnych usług należy zrezygnować z niektórych zabezpieczeń [1].

Konieczne jest znalezienie kompromisu między bezpieczeństwem, użytecznością, kosztami i wydajnością. Zaostrzenie środków bezpieczeństwa, ma przykład przez ograniczenie zakresu dostępnych usług czy wymaganie od użytkowników przeprowadzania procesu uwierzytelniania, obniża poziom użyteczności, może również prowadzić do spadku wydajności pracy systemu. Oprogramowanie zabezpieczające – dokonujące np. szyfrowania danych, wykrywające włamania, wyszukujące wirusy czy przeprowadzające kilkuetapowy proces logowania – wymaga zasobów systemowych. O wiele więcej mocy obliczeniowej potrzeba do przeprowadzenia sesji z wykorzystaniem protokołu SSL niż do dokonania tego bez szyfrowania. Spadki wydajności można zniwelować kupując droższe, wydajniejsze komputery lub maszyny przeznaczone specjalnie do szyfrowania.

Wydajność, użyteczność, koszty i bezpieczeństwo można postrzegać jako rywalizujące ze sobą elementy. Należy rozważyć wszystkie możliwości i wypracować sensowny kompromis między nimi. Biorąc pod uwagę wartość przechowywanych informacji, wielkość budżetu, oczekiwaną liczbę użytkowników oraz ich wymagania, trzeba znaleźć najlepsze rozwiązanie w tym zakresie [1].

Chcąc zminimalizować ryzyko ujawnienia informacji należy ograniczyć sposoby uzyskiwania do nich dostępu oraz określić grupę osób uprawnionych do ich przeglądania. Wiąże się z tym zaprojektowanie systemu w stosowny sposób, właściwie skonfigurowanie serwera, napisanie odpowiedniego oprogramowania, przetestowanie wszystkich

składników systemu, usunięcie niepotrzebnych usług serwera WWW oraz wykorzystanie mechanizmu uwierzytelniania. Projektowanie, konfiguracja, implementowanie oraz testowanie systemu, prowadzi do zmniejszenia ryzyka włamania oraz ogranicza prawdopodobieństwo wystąpienia błędu, który mógłby doprowadzić do ujawnienia przechowywanych informacji. Identyfikacji zagrożeń związanych z bezpieczeństwem przechowywanych danych i informacji oraz sposobom ich zapobiegania, poświęcony będzie niniejszy rozdział.

Wśród zagrożeń związanych z bezpieczeństwem magazynowanych danych można wymienić: [2]

- ujawnienie informacji poufnych,
- utratę bądź zniszczenie danych,
- modyfikacje danych,
- uniemożliwienie dostępu do danych.


*Rys.1. Zagrożenie dla danych firmy; źródło: http://itpedia.pl/images/b/b1/Back_1.jpg*

**Ujawnienie informacji poufnych**

Dane przechowywane w komputerze lub przesyłane pomiędzy jednym a drugim komputerem mogą być poufne. Charakter taki mają na przykład informacje dostarczone przez klienta, takie jak używane przez niego hasło dostępu, dane osobowe czy numer karty

kredytowej. Dane tego typu nie powinny być przechowywane na serwerze WWW, gdyż nie takie jest jego przeznaczenie. Serwer internetowy jest maszyną ogólnie dostępną co oznacza, że powinny być na nim magazynowane tylko informacje przeznaczone dla wszystkich lub te dane, które zostały właśnie przesłane przez użytkowników. Aby zmniejszyć liczbę potencjalnych słabych punktów systemu należy usunąć z niego także niepotrzebne usługi. W przypadku instalowania systemu Linux lub Windows NT jako systemu serwera sieciowego zostanie do niego dołączony cały zestaw usług, z których większość nie będzie wykorzystywana. Należy zatem je usunąć [3].

**Utrata lub zniszczenie danych**

Znacznie poważniejsze następstwa mogą wynikać z utraty danych, niż z ich ujawnienia. Przyczyną tego może być:

włamanie do systemu i sformatowanie twardego dysku,

usunięcie danych będące skutkiem błędu administratora lub programisty,

awaria dysku.

Aby temu zapobiec należy zabezpieczyć serwery przed atakiem ze strony crackerów, ograniczyć do niezbędnego minimum liczbę pracowników mających dostęp do systemu, wykorzystywać dyski wysokiej jakości. Zalecane jest stosowanie macierzy RAID (ang. *Redundant Array of Inexpensive Disks*), dzięki której kilka dysków funkcjonuje jak jeden szybszy i bardziej niezawodny nośnik danych. Istnieje tylko jeden niezawodny sposób ochrony przed utratą danych - **tworzenie kopii zapasowych**.

**Modyfikacje danych**

Modyfikacje mogą dotyczyć również plików z danymi lub plików wykonywalnych. Zastąpienie pliku wykonywalnego jego zmodyfikowaną wersją może umożliwić intruzowi nieograniczony dostęp do systemu lub pozwalać na nadanie szerszych uprawnień [4].

Jedną z metod zabezpieczania się przed tego typu działaniami jest obliczanie sumy kontrolnej dla danych przesyłanych w sieci. Umożliwia ona dokonywanie zmian przez kogoś nieuprawnionego, jednak porównując wyliczoną sumę kontrolną i porównując ją z sumą danych oryginalnych, można stwierdzić czy uległy one modyfikacji. Szyfrowanie danych również utrudnia dokonywanie w nich jakichkolwiek zmian.

W celu lepszej ochrony plików znajdujących się na serwerze przed zmianami ich zawartości należy wykorzystać możliwość nadawania uprawnień, udostępnianą przez system

operacyjny, i zabezpieczyć sam system przed dostępem z zewnątrz. Nadając odpowiednie prawa dostępu, można pozwolić użytkownikowi na korzystanie z danych zasobów systemu, ograniczając mu jednocześnie możliwość dokonywania zmian czy też modyfikacji plików należących do innych użytkowników. Brak możliwości określenia praw dostępu jest jedną z przyczyn, dla których Windows 95, Windows 98 i ME nie powinny być wykorzystywane jako systemy operacyjne serwerów [5].

Wykrycie dokonanych zmian jest bardzo trudne. Pliki wykorzystywane przez bazy danych do przechowywania zawartości tabel, podlegają ciągłym zmianom. Zarówno dane jak i programy mogą zostać zmienione. Dlatego właśnie modyfikacje istniejących danych stanowią jeszcze większe zagrożenie niż ich utrata.

**Uniemożliwienie dostępu do danych**

Użytkownicy w sytuacji, kiedy nie mogą spenetrować wybranej aplikacji, częsta starają się przeszkodzić innym w dostępie do danych. Ataki Denial of Service (DoS) przybierają różne formy: spowodowanie awarii serwera, generowanie obciążeń uniemożliwiających serwerowi odpowiadanie na żądania innych użytkowników [5].

Dostęp do serwera można zablokować poprzez:

spowodowanie awarii komputerów,

zapełnienie twardych dysków danymi, tak aby nie można było na nich zapisać nowych danych,

utworzenie tak wielu nowych procesów w komputerze, że zostanie zużyta cała dostępna pamięć; powoduje to spowolnienie działania uruchomionych procesów lub ich całkowite zablokowanie,

spowodowanie awarii sprzętowej serwera (na przykład w wyniku zniszczenia sterowników programowych),

przesyłanie do serwera tak dużych ilości danych, że nie może on właściwie rozpoznać ani obsłużyć przychodzącego ruchu sieciowego.

**Wstrzykiwanie złośliwego kodu**

Nowym rodzajem ataku rozpowszechniającym się w Internecie są wstrzyknięcia złośliwego kodu. Atakiem tego typu są tzw. skrypty krzyżowe (ang. *cross site scripting*) –

XSS, które nie powodują natychmiastowej utraty danych. Polegają na uruchomieniu kodu, który powoduje różne zniszczenia lub przekierowuje użytkowników w inne miejsca [5]..

Zasada działania skryptów XSS jest następująca:

Złośliwy użytkownik wykorzystuje formularz wyświetlający innym użytkownikom wprowadzone do niego dane (na przykład formularz do wpisywania komentarzy w internetowej tablicy ogłoszeń). Wprowadza tekst reprezentujący nie tylko wiadomość, ale również skrypt, który wykona się w przeglądarce klienckiej:

```
<sript>
document.location = ”idz.w_inne_miejsce?cookie=” + this.cookie;
<script>
```

Złośliwy użytkownik wysyła tak spreparowane dane i czeka.

Następny użytkownik, który przegląda tekst wprowadzony przez złośliwego użytkownika, uruchamia kod „wstrzykniętego” skryptu. W opisywanym przykładzie nastąpi przekierowanie użytkownika oraz przesłanie pliku *cookie* ze strony źródłowej.

### 2.1. Backup

Gromadzenie, przetwarzanie i analizowanie danych jest stałym i nieodłącznym elementem działalności każdej firmy i każdego przedsiębiorstwa. Dane elektroniczne składowane w aplikacjach biznesowych, e-biznesowych, w systemach bazodanowych oraz jako pliki użytkowników na dyskach serwerów są nieustannie narażone na utratę. Jak pokazują statystyki około 50% użytkowników systemów komputerowych nie stosuje żadnych zabezpieczeń, licząc że problem utraty danych ich nie dotyczy i nigdy ich nie spotka. Niestety prędzej lub też później, z różnych przyczyn przydarza się to każdemu. A po wystąpieniu awarii krytycznej najczęściej jest już za późno, koszt odtworzenia utraconych danych jest bardzo wysoki, a bardzo często danych tych już nie można odzyskać [3].

### 2.2. Archiwizacja danych

Archiwizacja danych polega na przenoszeniu na tańsze i bezpieczniejsze ale wolniejsze nośniki tych danych które są rzadko używane lub mają strategiczne znaczenie dla prawidłowego działania całego systemu informatycznego czy też firmy. Prawidłowo

skonstruowany proces archiwizacji danych winien udostępniać dane zarchiwizowane. W systemach wykorzystywanych do archiwizacji danych korzysta się najczęściej z magnetooptycznych i optycznych rozwiązań, ze względu na ich niski koszt i dużą pojemność [7].

Według statystyk ponad 80% archiwizowanych danych jest już później nie wykorzystywanych, lub korzysta się z nich bardzo rzadko. Rozwiązaniem pozwalającym przenieść dane na oszczędniejsze i wolniejsze nośniki danych jest HSM HSM (ang. *Hierarchical Storage Management*).

### 2.3. Kopia zapasowa

**Kopia zapasowa** to dodatkowe zabezpieczenie (*kopia*) nośników z backupem bądź zarchiwizowanymi danymi. Warto o niej pamiętać, bowiem taśmy, na których jest wykonywany backup, często są nadmiernie eksploatowane, a w wyniku tego ryzyko wykonania bezwartościowego (*bo bez możliwości odzyskania danych*) backupu znacznie rośnie.

### 2.4. Replikacja synchroniczna

Poprzez określenie replikacji synchronicznej należy rozmieć zabezpieczenie w czasie rzeczywistym danych. Podczas tworzenia, czy też modyfikowania zbioru danych tworzona jest ich kopia zapasowa np. w oddalonym centrum przetwarzania zapasowych danych. Metoda ta posiada ograniczenia wynikające z odległości pomiędzy centrum zapasowym, a podstawowym. Wprowadzono wiec replikację asynchroniczną polegającą na archiwizacji danych z kilkunastominutowym opóźnieniem [3].

### 2.5. Rodzaje backupów

#### 2.5.1 Backup całościowy (full backup)

**Backup pełny** polega na archiwizacji wszystkich danych, niezależnie od czasu, kiedy były one archiwizowane po raz ostatni. Czas wykonania kopii bezpieczeństwa jest przeważnie długi, ale ponieważ wszystkie potrzebne dane mogą być odzyskane z jednej tasiemki, czas potrzebny na uruchomienie serwera po awarii jest stosunkowo krótki. [9].

### 2.5.2 Backup przyrostowy (incremental backup)

**Backup przyrostowy** (incremental) jest najszybszym sposobem zrobienia kopii bezpieczeństwa, kopiowane są pliki, które zostały zmodyfikowane po ostatnim backupie pełnym lub przyrostowym. Czas jaki jest potrzebny do odtworzenia danych jest dłuższy niż w przypadku backupu pełnego i różnicowego, ale zwykle potrzeba do tego kilku tasiemek. [6].

### 2.5.3 Backup różnicowy (differential backup)

**Backup różnicowy** (differential) jest to tworzenie kopii zapasowej plików, które zostały zmodyfikowane po ostatnim pełnym backupie. Operacja kopiowania plików trwa stosunkowo krótko, rośnie w skali tygodnia. Za to odtworzenie systemu po takiej awarii trwa dłużej, bo zazwyczaj wymagane są do tego dwie kasety - z ostatniego tygodnia oraz najbardziej aktualna - z ostatniego dnia.

### 2.5.4 Backup lokalny

**Do zalety backupu lokalnego zaliczyć można:**

- Prostą instalację i konfigurację
- Stosunkowo niski czas wykonywania backupu
- Szybki transfer danych

**Wady:**

- Duży procent wystąpienia błędu ludzkiego
- Wzrastające koszta oprogramowania, sprzętu, administracji

- Koniczna codzienna ingerencja człowieka
- Utrudniony proces automatyzacji

### 2.5.5 Backup sieciowy

**Do zalety backupu sieciowego zaliczyć można:**

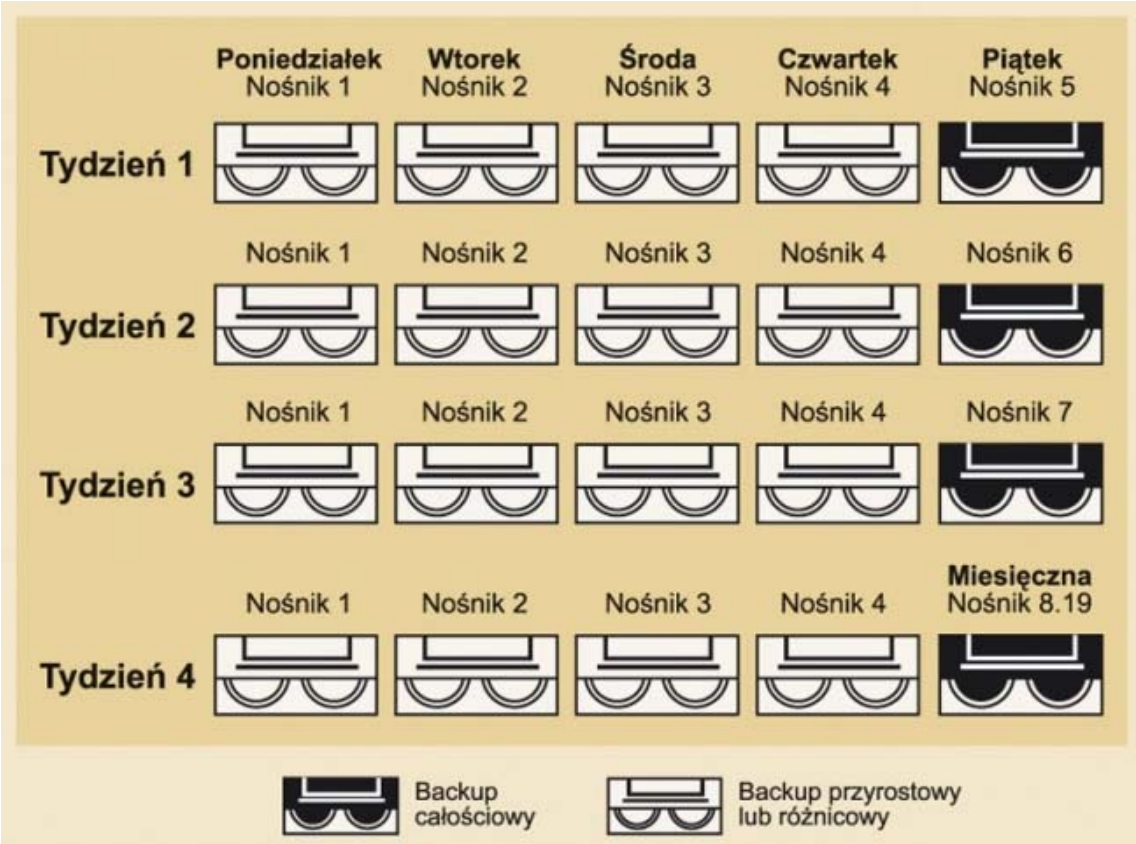
- Niski koszt administracji
- Łatwy proces automatyzacji
- Zarządzanie centralne

**Wady:**

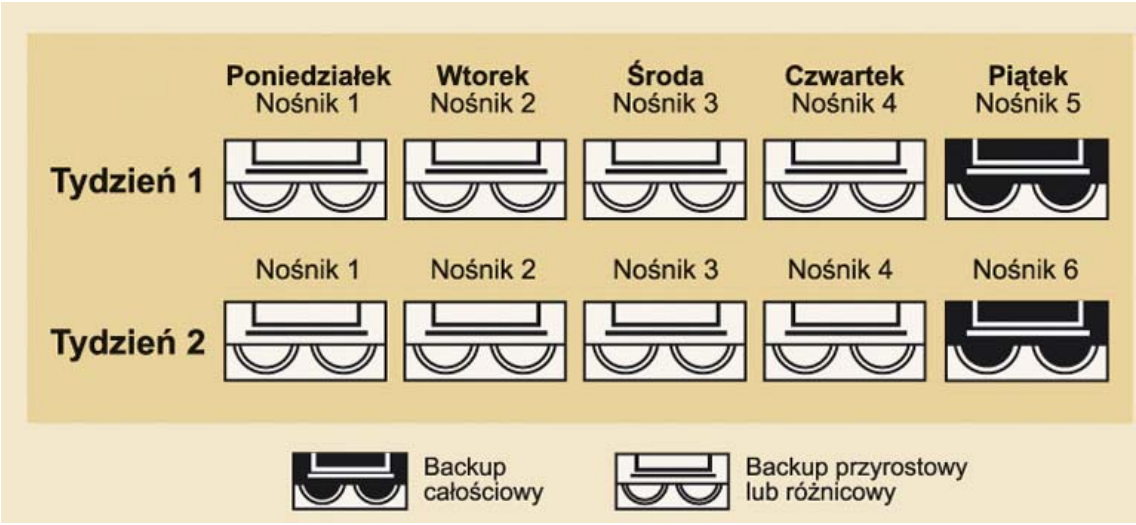
- Niski transfer danych
- Duże obciążenie zasobów sieciowych
- Długi czas potrzebny na wykonanie backupu
- Niskie wykorzystanie zasobów sprzętowych

## 2.6. Strategie backupu

**Strategia backupu Dziadek-Ojciec-Syn** zakłada iż wykorzystuje się 21 (dla 5-dniowego tygodnia pracy) taśm lub zestawów taśm. Cztery taśmy oznaczone są: poniedziałek, wtorek, środa, czwartek. Na których sporządzane będą przyrostowe lub różnicowe kopie danych. Kolejne pięć taśm należy oznaczyć: tydzień 1, tydzień 2, tydzień 3, tydzień 4, tydzień 5. Na nich z kolei powinno się sporządzić pełną kopię w każdy piątek. Pozostałych dwanaście taśm trzeba oznaczyć kolejnymi nazwami miesięcy. Na koniec każdego miesiąca należy na odpowiedniej tasiemce zapisać całkowitą kopię bezpieczeństwa danych. Taśmy z kopiami miesięcznymi powinny być przechowywane poza siedzibą firmy [5].



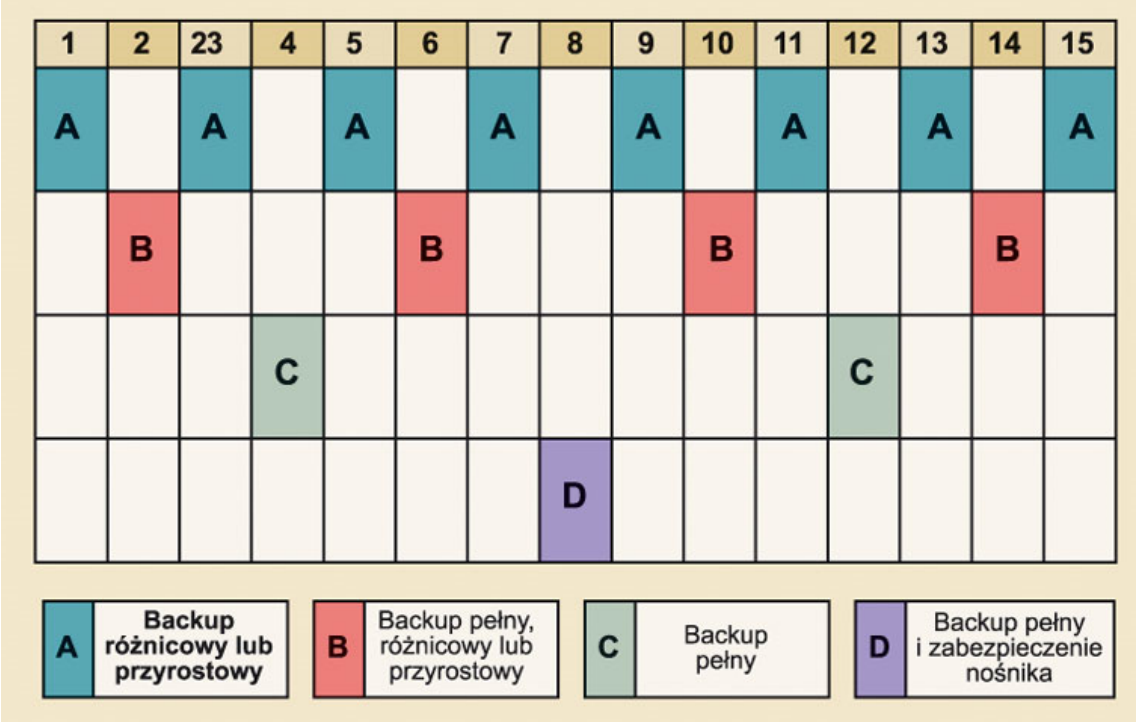

*Rys.2. Schemat typu „Dziadek/Ojciec/Syn”*




*Rys.3. Schemat typu „Ojciec/Syn”*

**Strategia backupu Wieża Hanoi** wymaga od osoby odpowiedzialnej za wykonywanie kopii bezpieczeństwa żelaznej konsekwencji, koncentracji i skupienia.

Zakłada wkroczenie nowego nośnika lub nowego zestawu nośników w sposób cykliczny. Należy pamiętać jednak, iż każdego kolejnego nośnika długość cyklu jest dwa razy dłuższa niż dla poprzedniego. W tej metodzie rotacji nośnik (lub zestaw nośników) A rozpoczyna schemat rotacji i jest wykorzystany w sposób cykliczny co drugi dzień. Drugi nośnik B jest dodawany do schematu rotacji w pierwszy wolny dzień, w którym nie jest wykorzystywany nośnik A i jest używany cyklicznie co czwarty dzień. Trzeci nośnik C jest dołączany do schematu rotacji w pierwszy wolny dzień, kiedy to nie jest wykorzystywany ani nośnik A, ani nośnik B, i jest używany cyklicznie co osiem dni. Do schematu rotacji można dołączać kolejne nośniki - D, E itd. Na nośnikach o najkrótszym cyklu znajdują się najbardziej aktualne kopie danych. Im dłuższy cykl zapisu danych na nośniku tym starsza kopia danych jest na nim zapisana. Tak jak w metodzie Dziadek-Ojciec-Syn, nośniki z długim cyklem zapisu danych należy przechowywać poza siedzibą firmy, aby uchronić je przed skutkami lokalnych katastrof [9].

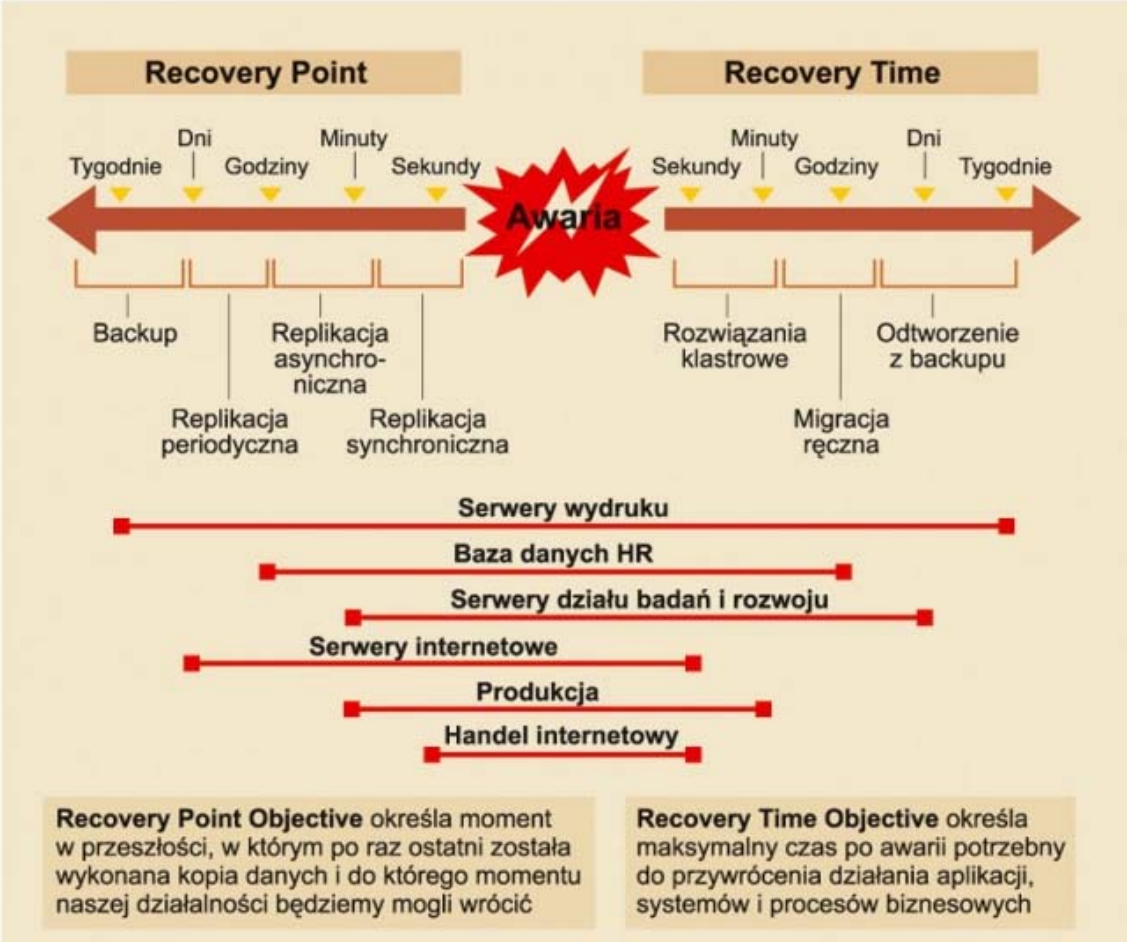



*Rys.4. Schemat typu „Wieża Hanoi”*

### 2.7. RPO i RTO

Tworząc politykę bezpieczeństwa w firmie zarząd winien wspólnie z informatykami określić następujące parametry:

- RPO (ang. Recovery Point Objetive);
- RTO (ang. Recovery Time Objective);



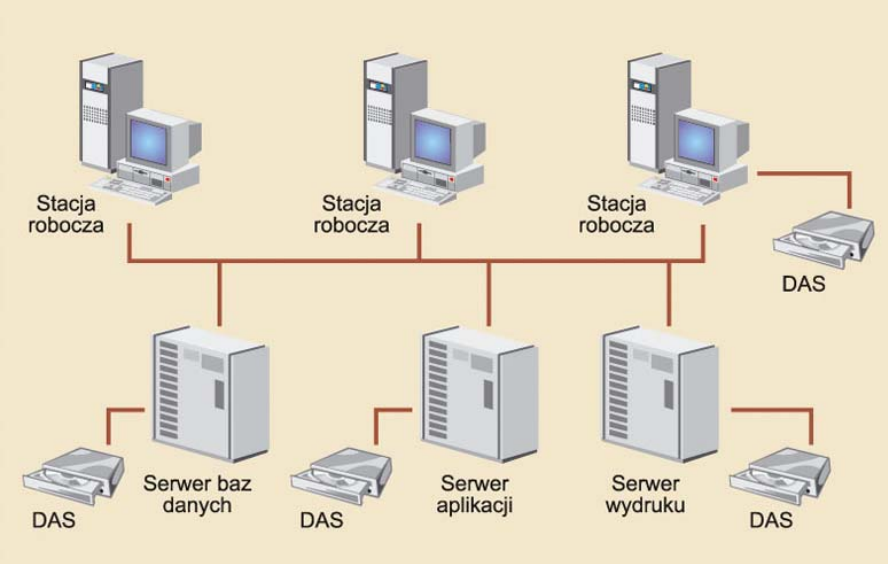

*Rys.5. RPO i RTO; źródło: http://itpedia.pl/index.php/RPO_i_RTO*

Parametr RPO określa moment w którym ostatni raz w firmie dokonano archiwizacji danych, i od tego momentu można przewrócić działalność firmy. Cze ten jest uzależniony od działalności firmy, gdyż w wypadku jednej wystarczy kopia zapasowa sprzed tygodnia , zaś w innym sprzed dosłownie kilku sekund (np. banki) [3].

Parametr RTO określa w jakim maksymalnie czasie można dokonać przywrócenia działania wszystkich systemów, aplikacji wykorzystywanych w firmie jak i jej procesów biznesowych.

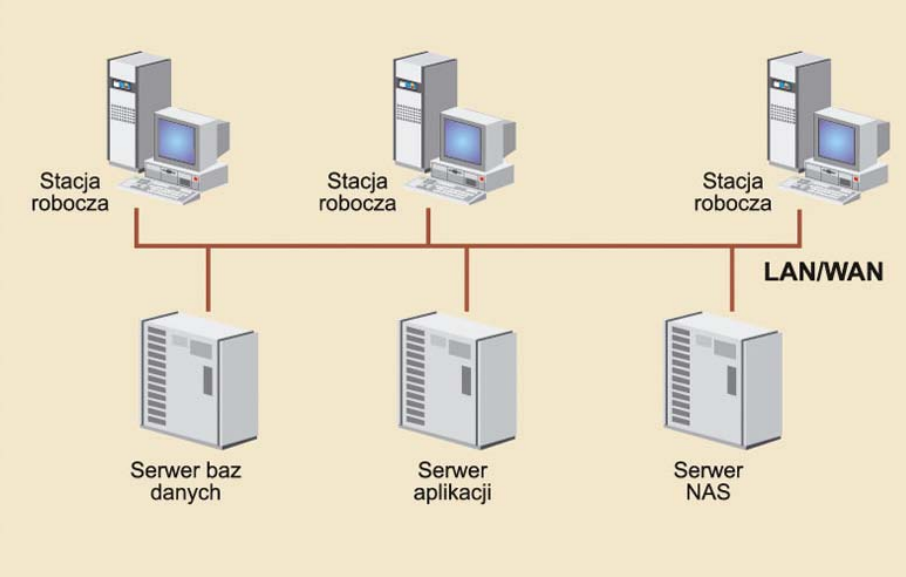
## 2.8. DAS, NAS, SAN

Firma przystępując do rozwiązania polegającego na wykorzystaniu pamięci masowych winna określić w jaki sposób będą udostępniane zasoby. Jednym z najpopularniejszych rozwiązań jest **DAS** (ang. *Direct Attached Storage*) polegający na bezpośrednim połączeniu pamięci masowej z komputerem, który jest odpowiedzialny za gromadzenie zebranych danych. Taki sposób zcentralizowania gromadzenia danych jest o tyle niewygodny, iż uniemożliwia efektywne w pełni kontrolowane zarządzanie pamięciami masowymi [1].



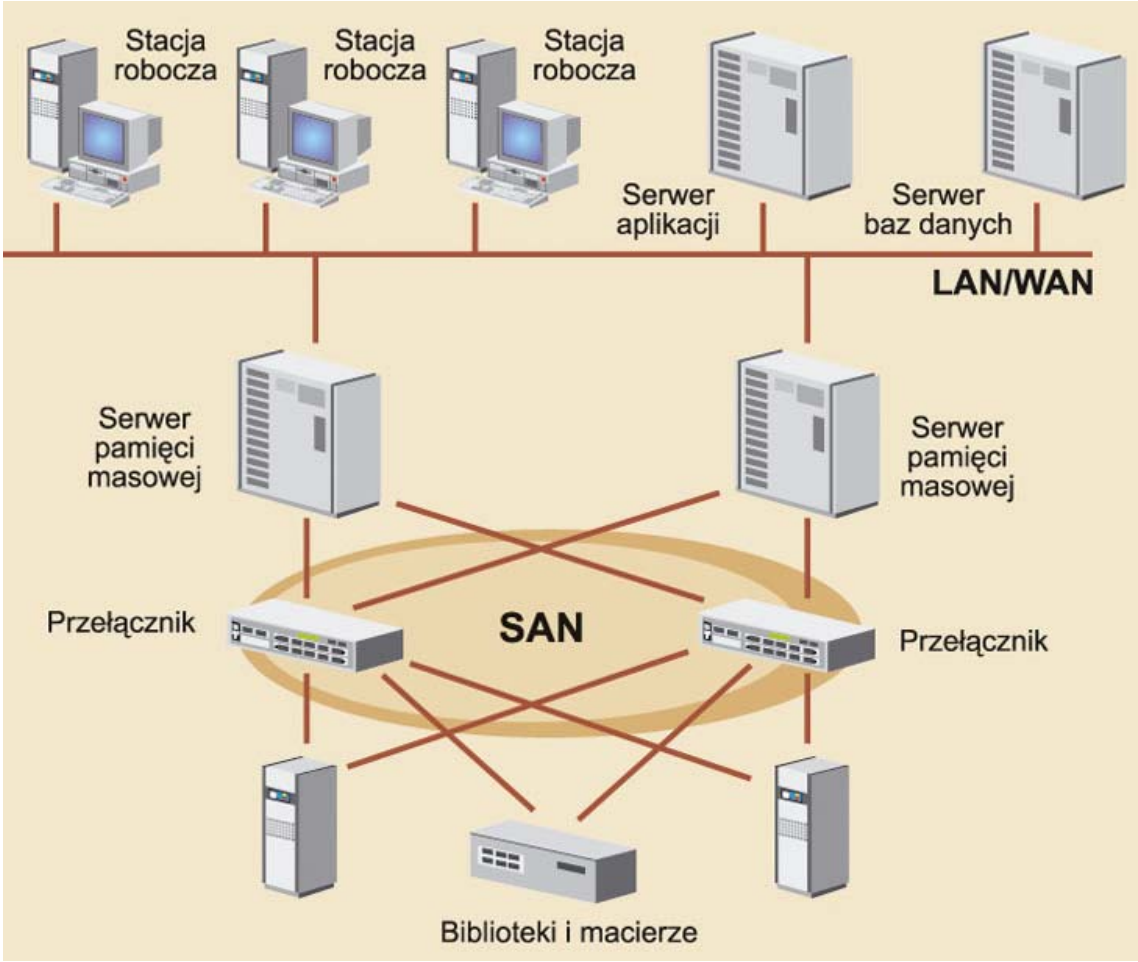

*Rys.6. Architektura DAS; źródło: http://itpedia.pl/index.php/DAS%2C_NAS_czy_SAN%3F*

Coraz częściej firmy decydują się na rozwiązanie **NAS** (ang. *Network Attached Storage*) polegające na podłączeniu urządzenia pamięci masowej do sieci Ethernet, który pozyskuje i udostępnia zasoby użytkownikom, którzy posiadają uprawnienia nadane przez administratora systemu. Podłączone w taki sposób dyski w macierze dyskowe mogą zostać połączone w RAID. Powoduje to odpowiednie zabezpieczenie i optymalizację wolnej przestrzeni dyskowej.




*Rys.7. Architektura NAS; źródło: http://itpedia.pl/index.php/DAS%2C_NAS_czy_SAN%3F*

Alternatywą wykorzystującą zaawansowane rozwiązania są sieci SAN (ang. *Storage Area Network*), które umożliwią nieograniczone podłączenie pamięci masowych. W skład budowy sieci SAN wchodzą nie tylko urządzenia pamięci masowych, ale także infrastruktura taka jak serwery i przełączniki [8].




*Rys.8. Architektura SAN; źródło: http://itpedia.pl/index.php/DAS%2C_NAS_czy_SAN%3F*

### 2.9. Rodzaje pamięci masowych i ich zastosowanie

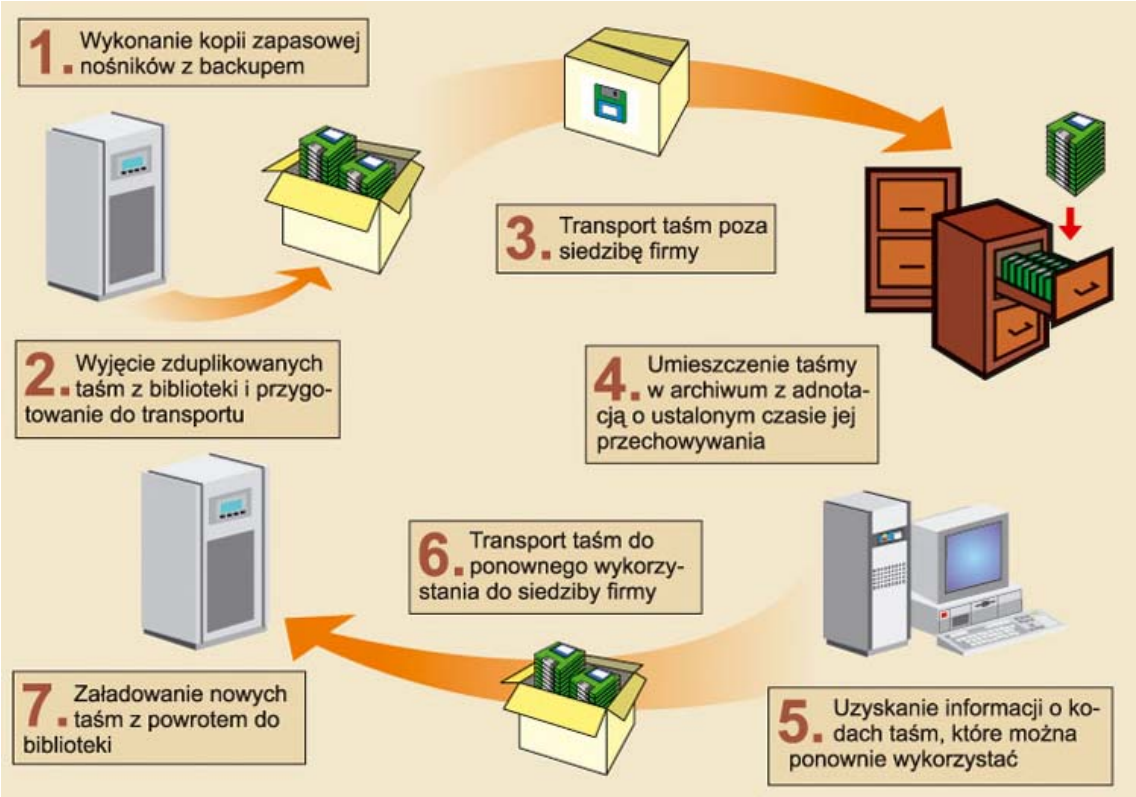
Do urządzeń umożliwiających bezpieczny backup danych można zaliczyć [5]:

- **streamer** – napęd taśmowy, który umożliwia odczyt i zapis danych na taśmie magnetycznej. Jego zaletą jest szybki transfer, zaś za wadę można uznać długi czas dostępu.
- **outoloader** – zmieniacz taśmowy, w skład którego wchodzi magazynek mogący pomieścić kilka taśm, automat które je zmienia oraz napęd.
- **biblioteka taśmowa** – urządzeni które zawiera jeden lub więcej napędów taśmowych, wyposażone w czytnik kodów kreskowych oraz system zaawansowanej robotyki odpowiedzialnej z obsługę magazynku z taśmami.

- **macierz dyskowa** – służy do zapisu danych które modyfikowane są na bieżąco, składa się ona z kilkunastu dysków twardych. Dyski łączone są w macierz RAID która może być pierwszego poziomu – zapis danych poprzez tworzenie ich lustrzanej kopii lub piątego poziomu – duplikowanie danych przy wykorzystaniu odpowiedniego algorytmu.

W zależności od czasu dostępu do danych, urządzenia pamięci masowych można podzielić według następującego kryterium [8]:

- **On-line storage - high performance –** w skład których wchodzą pamięci RAM – urządzenia tego typu charakteryzują się czasem dostępu który nie przekracza kilku milisekund. Najczęściej w rozwiązaniu storage służą do przechowywania indeksu bazy danych.
- **On-line storage –** w skład których wchodzą dyski twarde oraz macierze dyskowe – czas dostępu do tych urządzeń nie jest większy niż jedna sekunda. Ich zadaniem jest najczęściej przechowywanie baz danych, plików multimedialnych, aplikacji.
- **Near-line storage –** w skład których wchodzą dyski magnetooptyczne i optyczne – czas dostępu tych urządzeń sięga rzędu 30 sekund. Ich zadaniem jest przechowywanie danych, które nie są często używane.
- **Off-line storage –** w skład których wchodzą taśmy magnetyczne – czas dostępu do tych urządzeń sięga kilku minut. Wykorzystywane są do backupu tych danych które są najrzadziej wykorzystywane.
- **Off-line safety copy –** rozwiązanie które umieszcza nośniki z kopią backupowanych i archiwizowanych danych daleko od systemu informatycznego, zapewniając tym samym bezpieczeństwo danych firmy w czasie pożaru, powodzi, klęsk żywiołowych.



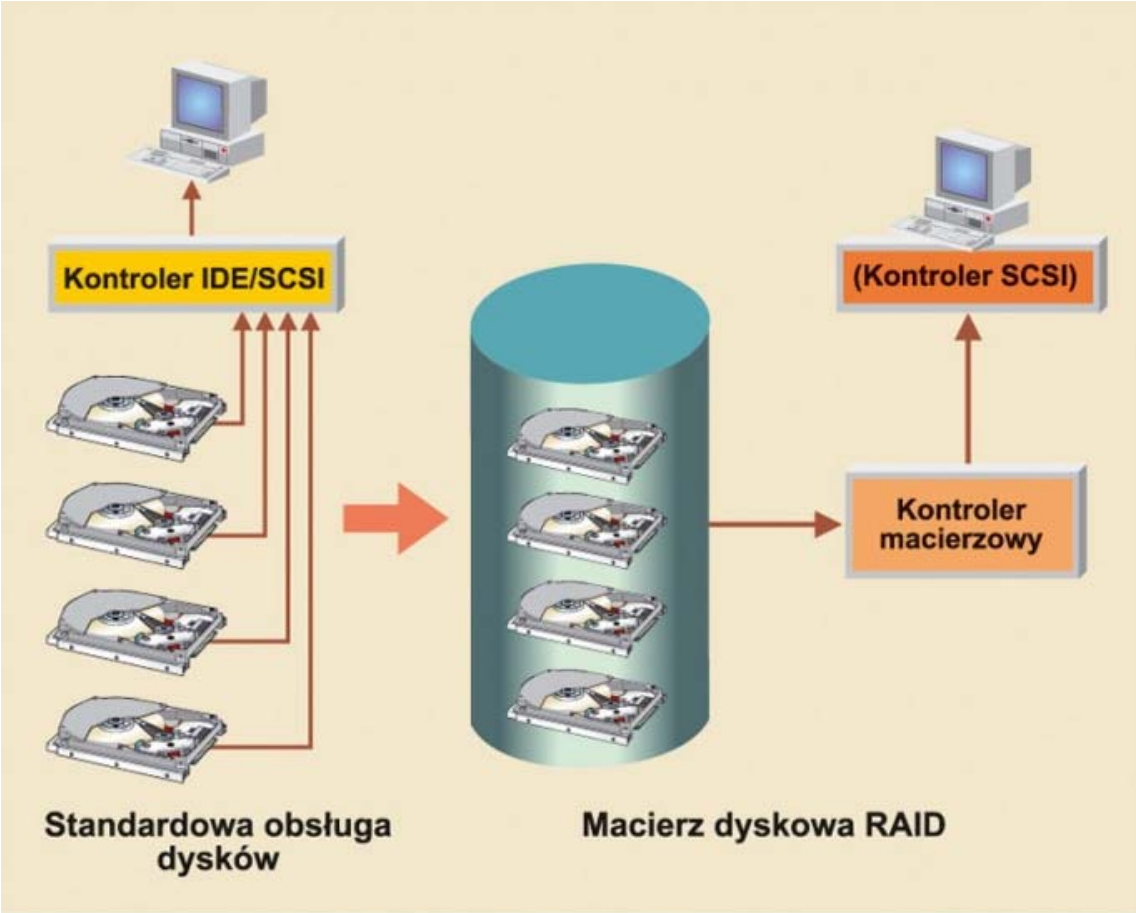

*Rys.9. Proces dystrybucji nośników poza siedzibą firmy*

### 2.10. RAID

W celu ochrony sytemu w czasie rzeczywistym przed utratą danych spowodowaną awarią dysku twardego należy zastosować RAID (ang. *Redundant Array Inexpensive Discs*).

W mniejszych systemach często stosowane są wewnętrzne kontrolery RAID SCSI lub RAID IDE. Pierwsze są bardziej wydajne, zaś drugie tańsze i mniej bezpieczne.

Firmy średniej wielkości winny stosować dyski wymienne w zewnętrznej obudowie lub macierze z zewnętrznymi kontrolerami RAID. Umożliwia to uniezależnienie proces działania macierzy od awarii systemowej. Wybierając macierz RAID należy kierować się odpowiednią wentylacją, systemem monitoringu temperatury czy też zdalnego zarządzania.




*Rys.10. Proces działania macierzy RAID*

W skład systemu ochrony danych w pamięciach masowych wchodzi:

1. Macierz RAID odpowiedzialna za zabezpieczenie systemu przed awarią dysków twardych;
2. System zapisu taśmowego chroniący przed ogólną awarią (*w tym całkowitą awarią macierzy RAID*), klęską żywiołową (*np. powódź, pożar*), a także umożliwia archiwizację danych; dzięki przechowywaniu backupów z różnych dni możemy odtworzyć stan np. sprzed awarii, która spowodowała niespójność danych;
3. dane, które nie podlegają zmianom i są rzadko używane, powinny być archiwizowane na urządzeniach optycznych lub magnetooptycznych, których nośniki są obecnie najtańsze w przeliczeniu na 1 GB. Na system zabezpieczania danych powinna składać się odpowiednia ochrona

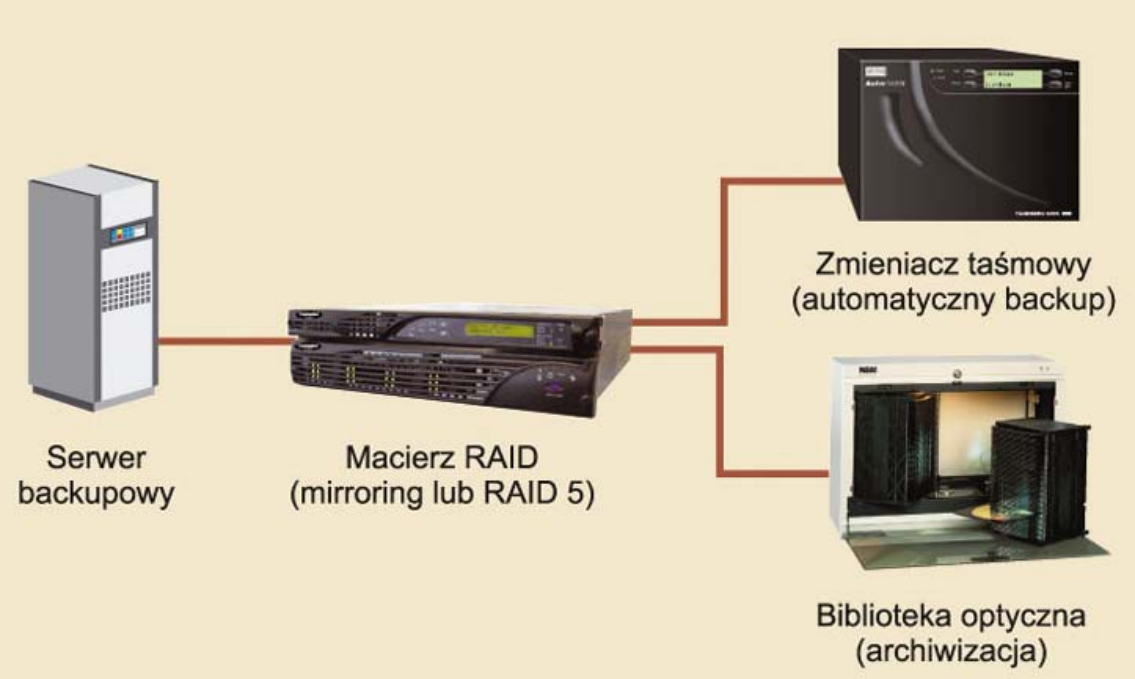
antywirusowa (*z mechanizmem automatycznej aktualizacji kodów wirusów*) i elektryczna.


*Rys.11. Rozwiązanie z zastosowaniem kontrolerów RAID*

Trzeba pamiętać o fakcie, że żaden system mirroringu czy replikacji nie zastąpi backupu. Tylko backup pozwala na spojrzenie wstecz i powrót do wersji danych sprzed określonego czasu. Daje to zabezpieczenie głównie przed wirusami lub błędami ukrytymi w programie bądź strukturze danych. Systemy redundancyjne, przy całej swojej doskonałości, naiwnie duplikują także wirusy czy wspomniane błędy.

W wielu przypadkach instalacja kompleksowego systemu bezpieczeństwa danych to duży wydatek. Nie trzeba ponosić go od razu i można poszczególne elementy rozwiązania zabezpieczania danych wdrażać etapami (*oczywiście, będąc świadomym wzrostu*

*zagrożenia utratą danych*). Decydując się na ten krok, warto jednak pomyśleć nad ścieżką rozwoju systemu i możliwościami jego rozbudowy. Inwestycja w rozwiązanie jednego, dużego i stabilnego producenta zagwarantuje, że rozbudowa systemu będzie łatwiejsza, a poszczególne jego elementy będą ze sobą kompatybilne. Mimo że wiele standardów w pamięciach masowych jest otwartych, to kompatybilność poszczególnych urządzeń pozostawia czasami wiele do życzenia.




*Rys.12. System backupu i archiwizacji danych*

# 3. Projekt backupu dla firmy średniej wielkości

Celem projektu jest stworzenie dokumentacji umożliwiającej, na jej podstawie wykonanie sieci komputerowej umożliwiającej backup danych dla średniej wielkości firmy programistycznej „XXX". Wspomniana firma zajmuje się produkcją różnego rodzaju programów komputerowych oraz projektowaniem portali internetowych.

W pracach nad projektem kierowano się przede wszystkim jakością i dużą niezawodnością projektowanej sieci, starano się aby sieć była otwarta na przyszłą rozbudowę przy optymalnych kosztach całej instalacji. Projekt obejmuje zakup zarówno sprzętu jak i oprogramowania.

## 3.1. Charakterystyka firmy

Opisywana firma działa w branży informatycznej jej zadaniem jest tworzenie oprogramowania. Głównym produktem firmy są portale internetowe, firma posiada również dział zajmujący się pisaniem oprogramowania. Języki wykorzystywane przez programistów to **JAVA** i **PHP**. W związku z tym konieczne jest zapewnienie niezbędnej infrastruktury teleinformatycznej i systemu archiwizacji danych.

Liczba pracowników zatrudnionych w firmie:

- Programiści aplikacji WEB (serwery FTP, HTTP, repozytoria kodów, bazy danych) – 20 osób;
- Programiści aplikacji okienkowych – 7 osób;
- Testerzy – 7 osób;
- Graficy – 2 osoby;
- Wdrożeniowcy – 5 osób;
- Administratorzy – 4 osoby;
- Kadrowcy – 2 osoby;
- Płace – 3 osoby;
- Marketing – 6 osób;

- Zarząd – 2 osoby;
- Sekretariat – 2 osoby;
- Handlowcy – 10 osób;
- Bazodanowcy – 2 osoby.

Firma posiada dwa budynki położone od siebie o 200 metrów. W jednym z nich znajduje się przestrzeń biurowa dla kadr, zarządu oraz sala konferencyjna. Pozostali pracownicy maja swoją siedzibę w drugim budynku (programiści, graficy, administratorzy, bazodanowcy, testerzy, wdrożeniowcy). Firma posiada swoją domenę internetową, w której utrzymuje strony WWW, oraz serwery poczty. W celu usprawnienia komunikacji planowane jest również wdrożenie usługi VoIP, tak aby wszyscy jej pracownicy byli ze sobą w stałym kontakcie, a także w celu obniżenia kosztów telefonicznych. Komunikacja wewnętrzna powinna uwzględniać również możliwość kontaktu poprzez komunikator tekstowy. Podczas projektowania sieci uwzględniono możliwość zatrudnienia przez firmę kolejnych pracowników

### 3.2. Założenia

Zadanie polegało na stworzeniu infrastruktury teleinformatycznej dla firmy z sektora IT z szybkim łączem internetowym, siecią lokalną opartą na technologii Gigabit Ethernet i łącza światłowodowe oraz wdrożeniem systemu serwerów backupowych umożliwiających archiwizację danych. Ze specyfiki działania systemu informatycznego takiej firmy wynika zarówno duża wymiana danych w sieci lokalnej jak i intensywna eksploatacja połączenia z Internetem.

W budynku dwukondygnacyjnym znajdować się będzie większość aktywnych urządzeń sieciowych tj. szafa krosownicza, serwery, router, sprzętowy firewall, acces point. Liczba punktów sieciowych obejmuje 114 stanowiska (72 stanowiska dla pracowników, 2 stanowiska dla sal konferencyjnych i 40 stanowisk dostępu bezprzewodowego dla sal konferencyjnych). Dodatkowo w większości pomieszczeń będą znajdować się nadmiarowe gniazda sieciowe, dzięki czemu przy dodawaniu nowych stanowisk komputerowych nie będzie potrzebna przebudowa sieci. W sumie budynek posiada 6 pomieszczeń

przeznaczonych dla użytku biurowego. W pomieszczeniu nr 107 umieszczona zostanie szafa 19” oraz sprzęt aktywny, będzie tu umieszczona serwerownia.

Planowane jest również utworzenie sal konferencyjnych w pomieszczeniach numer 004 i 205. W salach tych umieścimy cyfrowe projektory oraz punkty dostępowe WiFi.

Celem funkcjonalnym projektu jest przede wszystkim stworzenie niezawodnej, bezpiecznej, umożliwiającej łatwą rozbudowę nowoczesnej sieci komputerowej. Okablowanie zostanie tak poprowadzone by nie udało się przekroczyć odległości 100 metrów między PC a urządzeniem aktywnym, zgodnie ze standardami oraz tak aby nie narazić okablowania na uszkodzenia mechaniczne. Kable zostaną wyprowadzone w korytkach kablowych dzięki czemu ich przypadkowe uszkodzenie będzie trudniejsze a instalacja nie będzie szpecić pomieszczeń. Każdy kabel montowany zostanie zakończony gniazdkiem sieciowym kategorii 6 , które będzie odpowiednio opisane. Samo pomieszczenie z serwerami posiadać będzie kraty w oknach, solidne drzwi , instalację przeciwpożarową oraz klimatyzację.

Przed przystąpieniem do realizacji projektu zadano szefowi IT poniższe pytania w celu weryfikacji potrzeb backupu w firmie:

1. Czy przedsiębiorstwo robi backup wszystkich krytycznych danych co najmniej raz dziennie?
2. Czy kopie backupów firmy są przesyłane w ciągu 24 godzin do odległego bezpiecznego archiwum?
3. Czy niezależnie od wykonywania backupów jest dokonywana archiwizacja danych firmy przynajmniej ze względów formalnoprawnych?
4. Czy firma posiada wersje aplikacji zapewniające udostępnienie archiwów danych w przyszłości?
5. Czy jest planowane posiadanie odpowiednich napędów niezbędnych do odczytania danych archiwalnych za kilka (kilkanaście) lat?
6. Czy jest stosowana opcja weryfikacji zapisu? Czy jest ona na pewno uruchomiona w oprogramowaniu?
7. Czy jest testowana poprawność wykonywania backupów przez wyrywkowe odtwarzanie danych?

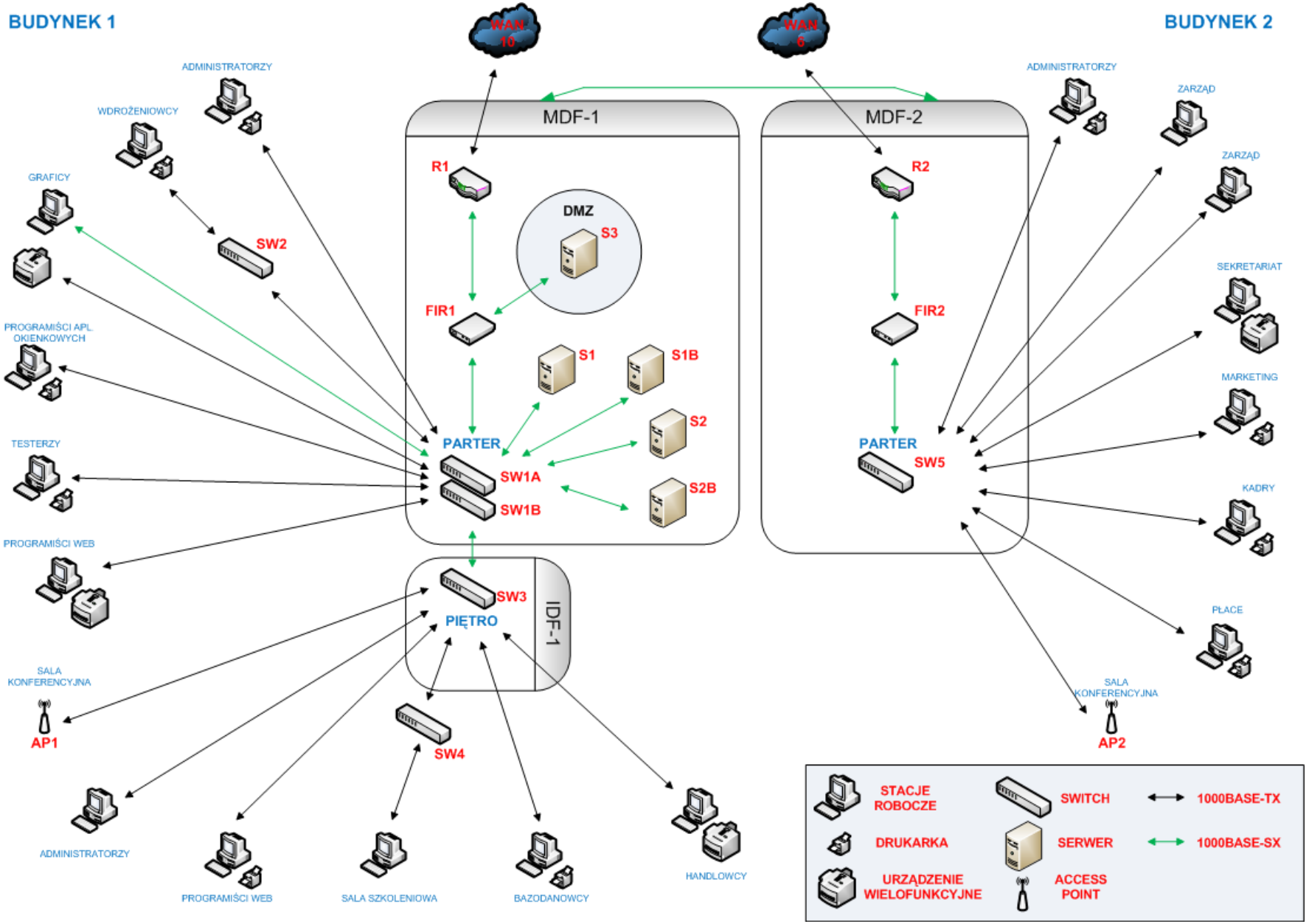
8. Czy jest stosowany odpowiedni schemat relacji mediów?
9. Czy firma ma dobrze zdefiniowany program wykonywania backupów: spisane procedury albo oprogramowanie do automatycznego backupu danych wykorzystującego odpowiednie biblioteki?
10. Czy stosowane systemy i procedury backupu spełniają obecne wymagania bezpieczeństwa w firmie?
11. Czy stosowany plan ochrony danych (Disaster Recovery) jest adekwatny do obecnych wymagań biznesowych?
12. Czy jest stosowane skalowalne, kompatybilne w przód i wstecz rozwiązanie backupowe, które uwzględnia przyrost danych?
13. Czy zaplanowano wzrost ilości danych w firmie w systemie backupowym?
14. Czy taśmy z backupem są właściwie transportowane, składowane, przenoszone i używane?
15. Czy stosowano algorytmy analizy ryzyka do oszacowania ryzyka finansowego przy usterce krytycznych funkcji systemu?
16. Czy precyzyjnie zdefiniowano kategorie ryzyka wraz z konsekwencjami (np. usterka zasilania, awaria aplikacji, awaria systemu komputerowego, awaria sieci Internet/Intranet, klęski żywiołowej) ?
17. Czy przedsiębiorstwo ma spisany plan postępowania w sytuacjach awaryjnych, zawierający procedury odtwarzania infrastruktury, systemów, backupów i archiwów?
18. Czy testowano w firmie plan ratunkowy w najgorszym przypadku?
19. Czy testy pokazały, że da się odtworzyć krytyczne funkcje biznesowe w założonym czasie?
20. Czy plan ratunkowy firmy jest regularnie korygowany zgodnie ze zmieniającymi się zasobami i wymaganiami biznesowymi?
21. Czy firma ma zunifikowany plan ratunkowy zawierający odległe centrum ratunkowe?
22. Czy firma zaimplementowała standardową i jednorodną technologię taśmową i oprogramowanie?

23. Czy zarząd uzgodnił wydatki i inne zasoby konieczne do stworzenia/utrzymania rozwoju systemu ratunkowego firmy?

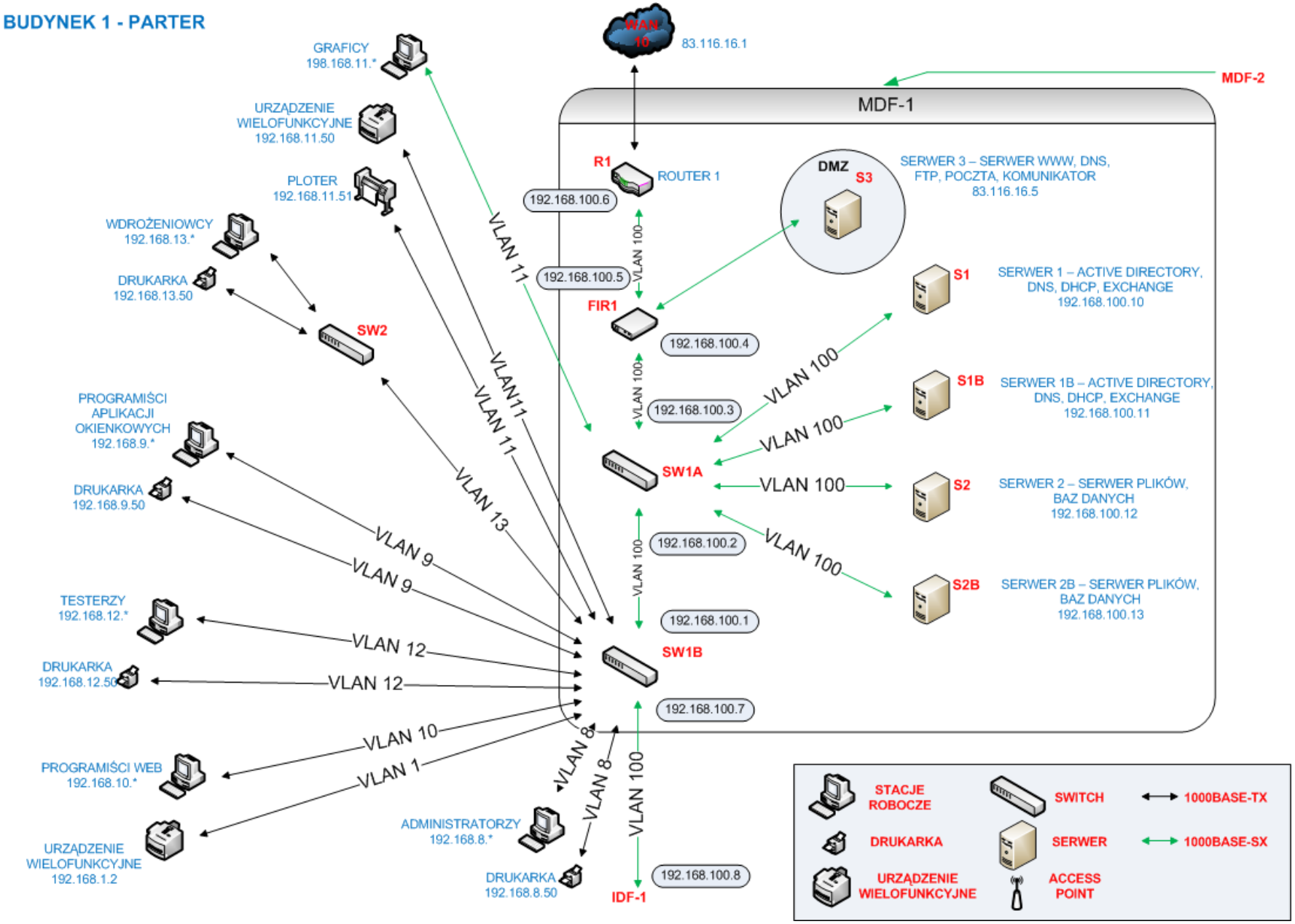
### 3.3. Sieć logiczna

Budynki połączone są ze sobą kablem światłowodowym 12 włóknowym MM 62,5/125µm OM3, LSZH, luźna tuba firmy Molex Premise Networks co pozwoli na uzyskanie odpowiedniej przepustowości łącza tj. 2Gb/s (wykorzystując 4 włókna).

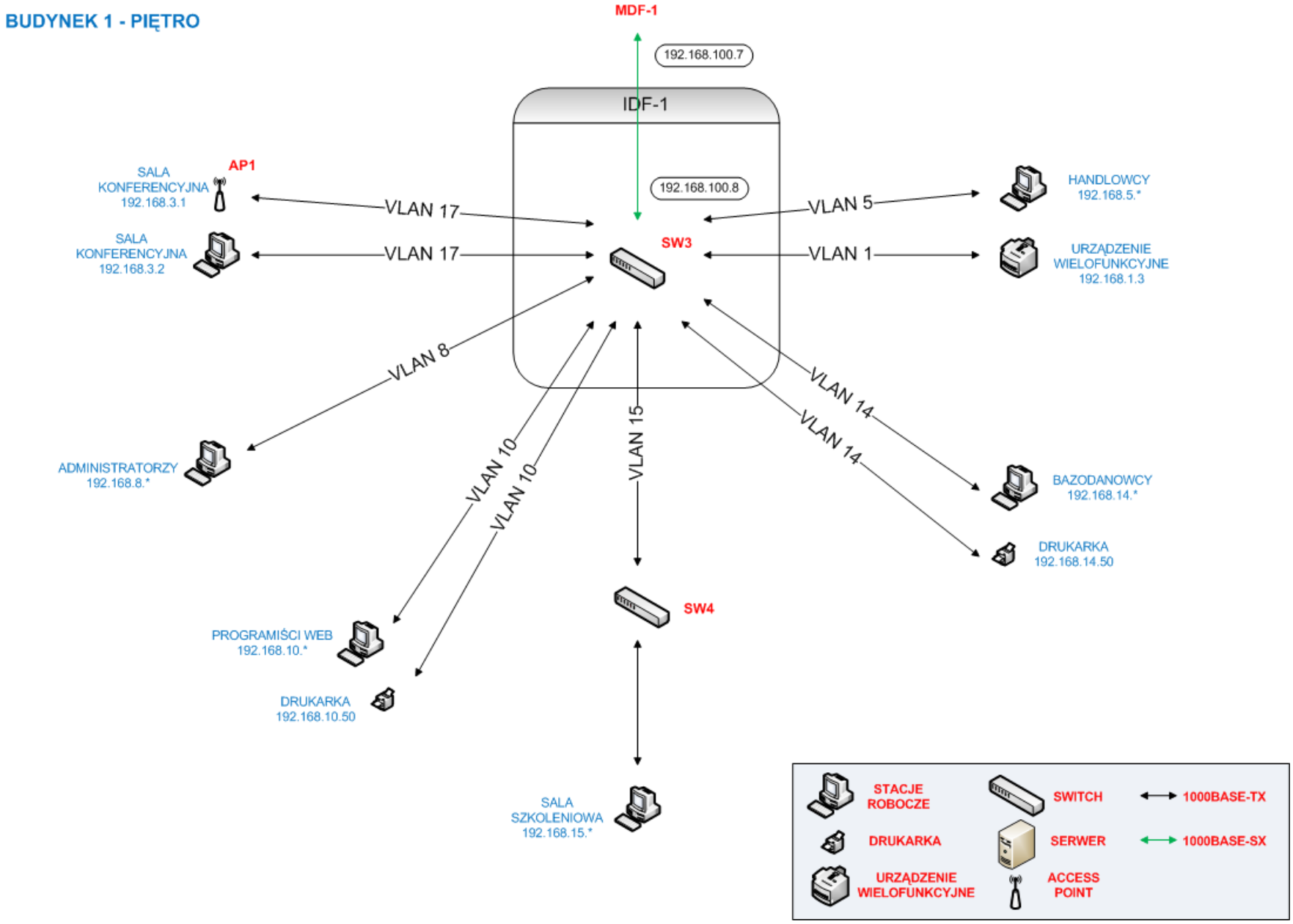
W obydwu budynkach sieć LAN ma topologię gwiazdy hierarchicznej, której centralnymi miejscami są główne punkty dystrybucyjne: MDF-1 dla budynku 1 i MDF-2 dla budynku 2. Pośrednim punktem dystrybucyjnym w budynku 1 jest IDF-1 mieszczący się na piętrze. Punkty dystrybucyjne MDF-1 i MDF-2 pełnią podwójną rolę – są głównymi punktami dystrybucyjnymi dla swych budynków i jednocześnie lokalnymi punktami dystrybucyjnymi dla swojej kondygnacji. Z MDF-1 rozprowadzone jest okablowanie poziome na parterze budynku 1, natomiast MDF-2 obsługuje budynek 2. Dzięki organizacji hierarchicznej, która jest najlepszym rozwiązaniem dla sieci LAN o rozmiarach średnich lub dużych, rozwiązane są problemy skalowalności i agregacji ruchu w sieci. Na brzegach sieci obydwu budynków pracują routery Cisco 3825DC, które zapewniają połączenie ze światem zewnętrznym. W budynku nr 1 należy wyróżnić 2 główne switche wchodzące w skład MDF-1: SW1A – Cisco WS-C3750G-12S-S, który posiada 12 gniazd SFP; oraz Cisco WS-C3560G-48PS-S posiadający 48 portów 1000BASE-TX i 4 porty SFP. Taka konfiguracja umożliwia pracę w całej sieci z wyższą niż standardowa przepustowością i pozwala na jej przyszłą rozbudowę. Do switcha SW1A za pomocą światłowodu podłączone są: serwery S1, S1B, S2, S2B; firewall FIR1 (z kolei do firewalla podłączone są: router R1 i serwer S3); stacje robocze grafików; switch SW1B; switch SW5 który znajduje się w budynku 2. Pozostałe połączenia zostały wykonane za pośrednictwem kabli UTP Molex PowerCat6 LSZH.



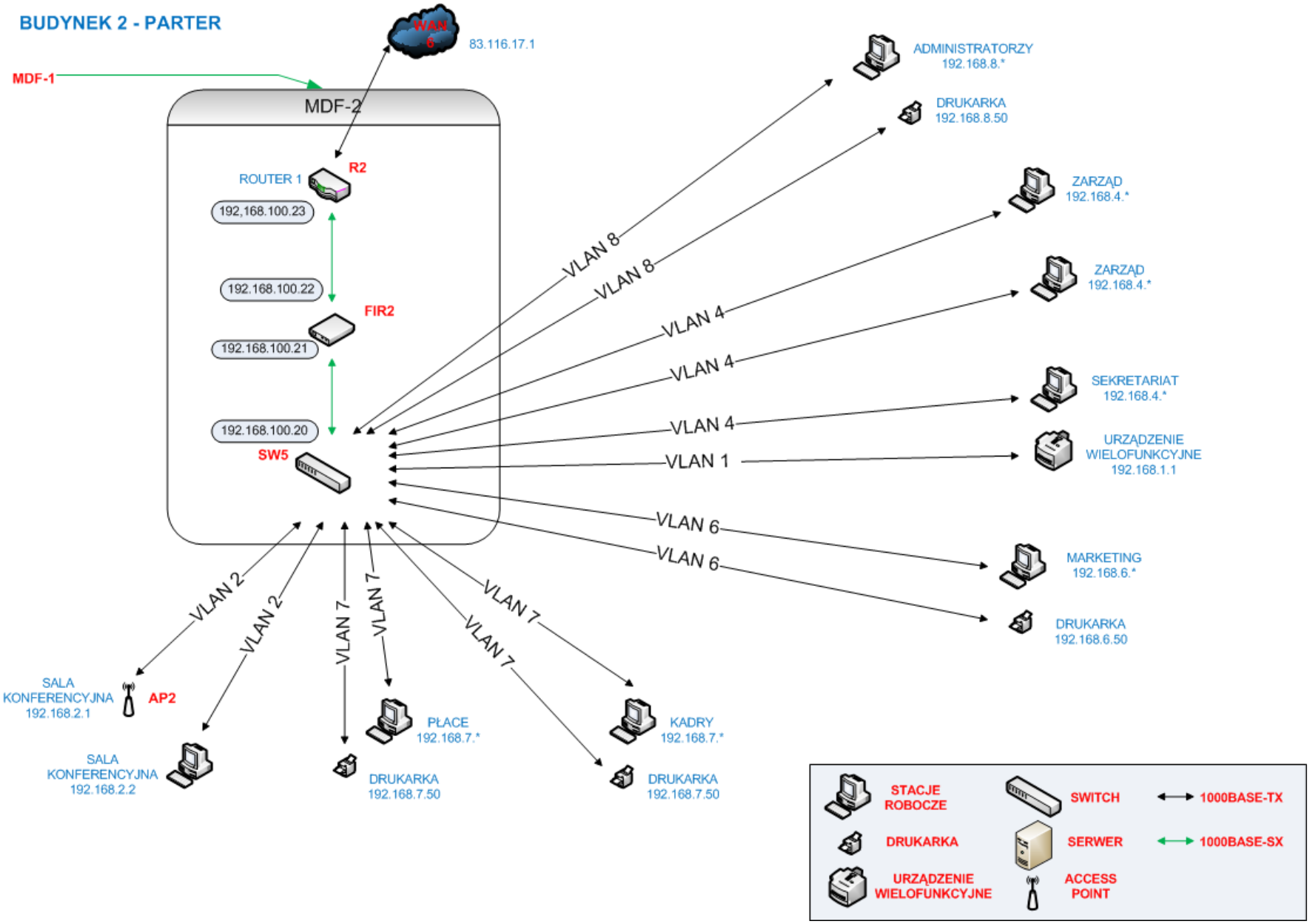

*Rys.13. Schemat sieci – budynek 1*




*Rys.14. Schemat sieci – budynek 1parter*




*Rys.15. Schemat sieci – budynek 1- I piętro*




*Rys.16. Schemat sieci – budynek 2*

### 3.4. Zestawienie serwerów do backupu

Projekt wymaga, aby dobierając serwery fizyczne były one bardzo szybkie, bezawaryjne i mocno rozbudowane z sieciowym systemem operacyjnym, świadczące klientom różne usługi. Główny nacisk w zakresie bazy sprzętowej postawiono na bezpieczeństwo – odporność na uszkodzenia, czyli zdolność do kontynuowania pracy pomimo uszkodzenia istotnych podsystemów, stabilność pracy wykorzystywanych urządzeń.

Przy projektowaniu sprzętowym serwerów wzięto też pod uwagę to, żeby to był sprzęt solidny z zapasem wydajności, który pozwoli uniknąć drogich, doraźnych modernizacji oraz umożliwi pracę w warunkach nieprzewidzianych skokowych wzrostów natężenia ruchu w sieci. Pomyślano także, aby miał zapewnioną skalowalność, która ma możliwość adaptacji sprzętu dla rosnących potrzeb rozwojowych firmy i był zgodny z obecnymi standardami.

W firmie znajduje się łącznie 5 serwerów, na każdym z nich działają konkretne usługi pod odpowiednio dobranym systemem operacyjnym.

Serwery główne tj: S1, S1B, S2, S2B pracują na systemach Windows 2003 Server Enterprise natomiast serwer S3 na systemie Linux Slackware.

Funkcje i usługi poszczególnych serwerów:

- S1 – Active Directory, DNS, DHCP, Exchange
- S1B – Active Directory, DNS, DHCP, Exchange
- S2 – jest serwerem plików oraz baz danych
- S2B – jest serwerem plików oraz baz danych
- S3 – WWW (Apache), DNS, FTP, Poczta (Postfix), Komunikator (X-Lite)

**Serwer plików**

Serwer plików przechowuje i zabezpiecza dane oraz udostępnia pliki i katalogi innym użytkownikom sieci. Może też przechowywać foldery macierzyste użytkowników, profile mobilne, foldery z aplikacjami czy sterowniki.

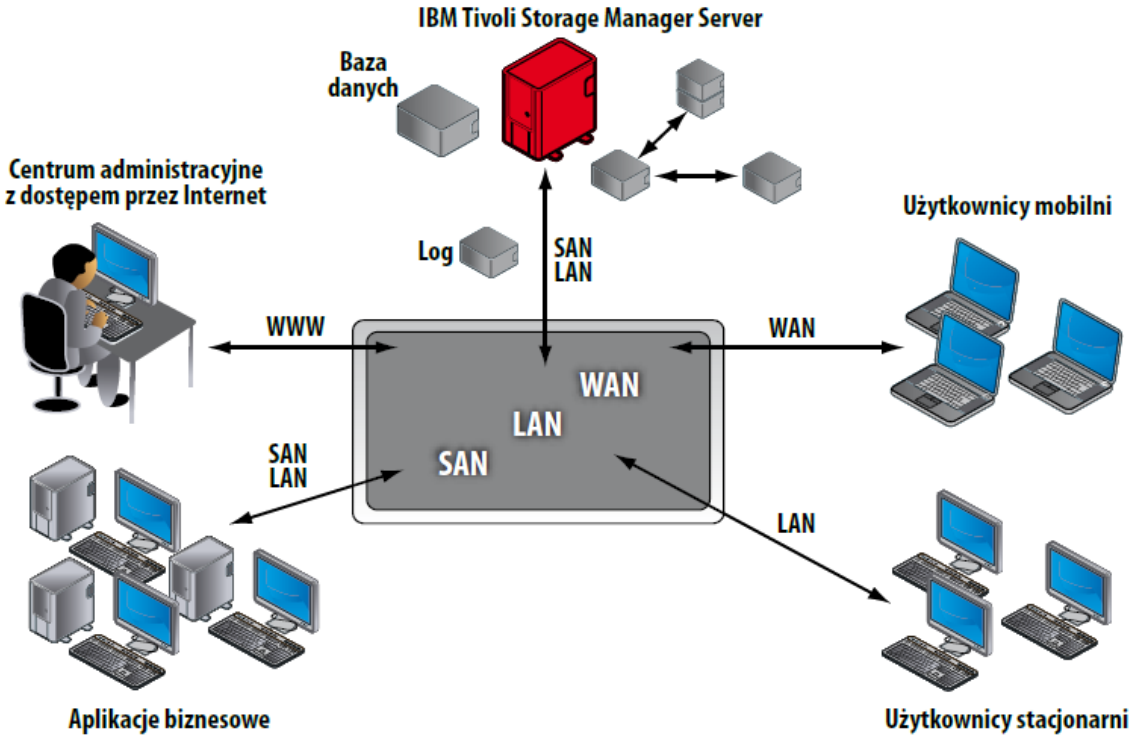
Należy zwrócić szczególną uwagę iż serwery S1 i S1B pełnią te same funkcje, spowodowane jest to tym, że serwer S1B jest serwerem backupowym serwera S1. Są to

zupełnie odrębne maszyny z własnymi systemami operacyjnymi, ale działają na wspólnej zewnętrznej macierzy dyskowej, na której znajdują się dane. Jest to bardzo dobre rozwiązanie, ponieważ w sytuacji gdy awarii ulegnie serwer S1, jego rolę przejmuje zastępczy - S1B. Analogicznie sprawa się ma z serwerami S2 i S2B. Macierze zewnętrzne wykorzystane w projekcie pracują w trybie RAID 5, co gwarantuje wysokie bezpieczeństwo danych. RAID 5 pracuje bardzo podobnie do poziomu czwartego z tą różnicą, iż bity parzystości nie są zapisywane na specjalnie do tego przeznaczonym dysku, lecz są rozpraszane po całej strukturze macierzy. RAID 5 umożliwia odzyskanie danych w razie awarii jednego z dysków przy wykorzystaniu danych i kodów korekcyjnych zapisanych na pozostałych. Oferuje większą prędkość odczytu niż mirroring ale przy jego zastosowaniu nieznacznie spada prędkość zapisu. Poziom piąty jest całkowicie bezpieczny dla danych - w razie awarii system automatycznie odbuduje utracone dane, tak by mogły być odczytywane, zmniejszając jednak bieżącą wydajność macierzy. Spowolnienie jest chwilowe. Po zamontowaniu nowego dysku i odtworzeniu danych wydajność macierzy wraca do normy.

### 3.4.1. Proponowane rozwiązanie

Na potrzeby backupu zostanie zaimplementowany system IBM Tivoli Storage Manager umożliwiający:

- Odzysk danych po awarii;
- Zabezpieczenie danych na wypadek katastrofy;
- Pełne zabezpieczenie aplikacji działających online oraz baz danych;
- Profesjonalne zarządzanie powierzchnią dyskową;
- Ochrona danych backupowych;
- Optymalizacja całego systemu backupowego pod kątem czasu odtworzenia i zabezpieczenia danych;
- Automatyzacja procesu przywracania danych i przeprowadzanie backupu;




*Rys.17. IBM Tivoli Storage Menager*

**Korzyści:**

- odporność na awarię jednego dysku
- zwiększona szybkość odczytu - porównywalna do macierzy RAID 0 złożonej z N-1 dysków

**Wady:**

- w przypadku awarii dysku dostęp do danych jest spowolniony z powodu obliczeń sum kontrolnych

### Serwer S1, S1B, S3

1U Intel dual CPU serwer Thomas Krenn SC811

*Rys.18. 1U Intel dual CPU serwer Thomas Krenn SC811*

**Obsługiwane procesory**

- 2x Intel® Xeon 5xxx
- FSB 1333 MHz
- Cache L2 8192 KB

**Pamięć RAM**

- 6 GB DDR2 667/533 MHz unbuffered ECC Registered
- Dual channel memory bus
- DDR2 fully buffered DIMM

**Płyta główna**

- SuperMicro X7DVL-E
- Intel® 5000V
- Kontroler IDE on-board
- Kontroler SATA RAID on-board (RAID 0,1; tylko pod systemem Windows)

**Dyski twarde**

- SATA
- maks. 2 szt.
- Hot-swap Backplane 2x Backplane
- Chipset Intel® 5000V

**Gniazda rozszerzeń**

- 1x 64-bit 133/100 MHz PCI-X LAN 2x Gigabit LAN on-board Urządzenia on-board
- 1x VGA (ATI ES1000 Graphics, 16 MB)
- 1x Fast UART 16550 serial port

- 1x ATA/100 EIDE channel
- 2x PS/2 - mysz, klawiatura
- 6x USB 2.0 compliant / 1.1 compatible (4x internal USB, 2x rear ports)

**Zarządzanie serwerem**

- Super Doctor III
- System zarządzania i nadzoru Super Doctor III (Supermicro)
- Narzędzie webowe, umożliwiające zdalny dostęp do serwera przez IP, bez dodatkowego sprzętu
- Możliwość monitorowania krytycznych parametrów systemu (temperatura CPU, obciążenie systemu, stan coolerów i zasilaczy, etc.
- Automatyczne e-mailowe powiadomienia o zdarzeniach krytycznych
- Wsparcie protokołu SNMP (Simple Network Management Protocol) SATA RAID on-board
- 6 portów;
- RAID 0,1,5,10
- Wymiary 1Ux 427x 574 mm (WxSxG
- Waga 15 kg (konfiguracja standardowa)
- Głośność 64/65 dBA (w odległości 1,0 m; tryb czuwania/pełne obciążenie)

**Konfiguracja:**

- Procesor: 1x Quad-core Intel Xeon X5420 2,50GHz 12MB FSB1333
- RAM: 8192 MB ECC Reg. DDR2 667 MHz ATP FB-Dimm (4x 2048 MB)
- Dyski: 2x 500 GB SATA II Western Digital Raid Edition 2 Green Power
- Kontroler: Qlogic QLA2462 Fibre Channel HBA
- Napęd: Slim DVD-ROM
- Zasilacz: 2x 520 Watt

**Serwer S2, S2B - 1U Intel dual CPU serwer Thomas Krenn 6015**

*Rys.19. 1U Intel dual CPU serwer Thomas Krenn 6015*

**Obsługiwane procesory**

- 2x Intel® Xeon 5xxx
- FSB 1333 MHz
- Cache L2 12 MB

**Pamięć RAM**

- maks. 16 GB DDR2 667/533 MHz unbuffered ECC Registered
- Dual channel memory bus
- DDR2 fully buffered DIMM

**Płyta główna**

- SuperMicro X7DBR-3
- Intel® 5000P (Blackford)
- Kontroler IDE on-board
- Kontroler SATA RAID on-board (RAID 0,1,5,10; 6 portów, tylko pod systemem Windows)
- Kontroler SAS RAID on-board (RAID 0,1,10; tylko pod systemem Windows)

**Dyski twarde**

- SATA/SAS
- maks. 4 szt.
- Hot-swap Backplane 4x Backplane SATA II/SAS

**Gniazda rozszerzeń**

- 2x PCI-Express (x8)
- 2x 64-bit 133/100 MHz PCI-X LAN 2x Gigabit LAN on-board Urządzenia on-board
- 1x VGA (ATI ES1000 Graphics, 16 MB)
- 1x Fast UART 16550 serial port

- 1x ATA/100 EIDE channel
- 2x PS/2 - mysz, klawiatura
- 5x USB 2.0 compliant / 1.1 compatible (3x internal USB, 2x rear ports)

**Zarządzanie serwerem**

- Super Doctor III
- System zarządzania i nadzoru Super Doctor III (Supermicro)
- Narzędzie webowe, umożliwiające zdalny dostęp do serwera przez IP, bez dodatkowego sprzętu
- Możliwość monitorowania krytycznych parametrów systemu (temperatura CPU, obciążenie systemu, stan coolerów i zasilaczy, etc.)
- Automatyczne e-mailowe powiadomienia o zdarzeniach krytycznych
- Wsparcie protokołu SNMP (Simple Network Management Protocol) SATA RAID on-board
- 6 portów;
- RAID 0,1,5,10
- Wymiary 1Ux 437x 650 mm (WxSxG
- Waga 20 kg (konfiguracja standardowa)

**Konfiguracja:**

- Procesor: 2x Quad-core Intel Xeon X5420 2,50GHz 12MB FSB1333
- RAM: 16384 MB ECC Reg. DDR2 667 MHz ATP FB-Dimm (8x 2048 MB)
- Dyski: 4x 147 GB SAS Fujitsu MBA3147RC 15k obr/min
- Kontroler: Qlogic QLE2462-CK (Fibre Channel HBA)
- Napęd: Slim DVD-ROM
- Zasilacz: 2x 650 Watt (hot-swap)

**MACIERZ DYSKOWA DLA SERWERÓW S1 I S1B -**2U ES6612 SATA system RAID

System RAID w obudowie 2U z maks. 12 dyskami twardymi. Interfejs SCSI lub Fibre Channel

*Rys.20. ES6612 SATA system RAID*

**Informacje techniczne:**

- Maksymalnie 12 dysków twardych (pojemność macierzy do 9 TB)
- Kontroler z procesorem Intel 80321, do dyspozycji RAID 6
- RAID 0,1,0+1,3,5,6,JBOD
- Dyski twarde hot-spare
- Redundantne zasilacze i wentylatory
- Zarządzanie systemem poprzez wbudowany serwer werbowy (port Ethernet)

**Konfiguracja:**

System: EUROstor system RAID 2U SATA ES-6612F4 (FC/SATA)

Cache: 1024 MB

Konektor: Fibre Channel 4GB/s (SFP)

Dyski: 4x 1000 GB SATA II Western Digital Raid Edition 2

**MACIERZ DYSKOWA DLA SERWERÓW S2 I S2B -** 2U ES6612 SAS SYSTEM RAID

System RAID w obudowie 2U z maks. 12 dyskami twardymi. Interfejs SAS lub Fibre Channel

*Rys.21. 2U ES6612 SAS SYSTEM RAID*

**Informacje techniczne:**

- Maksymalnie 12 dysków twardych (pojemność macierzy do 9 TB)
- Kontroler z procesorem Intel 80321, do dyspozycji RAID 6
- RAID 0,1,0+1,3,5,6,30,50,60,JBOD
- Dyski twarde hot-spare
- Redundantne zasilacze i wentylatory
- Zarządzanie systemem poprzez wbudowany serwer werbowy (port Ethernet)

**Konfiguracja:**

System: EUROstor System RAID 2U SAS ES-6612SF (FC/SAS)

Cache: 2048 MB

Konektor: Fibre Channel 4GB/s (SFP)

Dyski: 4x 300 GB SAS Fujitsu MBA3300RC 15k obr/min

### 3.5. Adresacja sieci

Cała sieć lokalna będzie funkcjonować w prywatnej puli adresów klasy C. Są to adresy prywatne, które mogą być wykorzystane tylko w sieciach lokalnych, a za sprawą techniki maskowania adresów sieciowych NAT na routerach wszystkie komputery będą miały wyjście na publiczną część Internetu.

Aby ujednolicić przydzielanie adresów IP zaproponowano następujący schemat adresowania:

- Sieć 192.168.A.B, gdzie
    - Pierwsze 2 oktety (192.168) oznaczają, że wszystkie hosty z sieci wewnętrznej będą funkcjonowały w prywatnej sieci klasy C.
    - A oznacza kolejne grupy pracowników i urządzeń, a zarazem numery kolejnych VLANów, przy czym:

        - 1 (192.168.1.*) dla współdzielonych zasobów dostępnych dla wszystkich grup (głównie dla dużych kombajnów typu drukarka/skaner/kopiarka
        - 2 (192.168.2.*) sala konferencyjna I
        - 3 (192.168.3.*) sala konferencyjna II
        - 4 (192.168.4.*) dla sekretariatu i zarządu
        - 5 (192.168.5.*) dla handlowców
        - 6 (192.168.6.*) dla działu marketingu
        - 7 (192.168.7.*) dla działu kadry i płace
        - 8 (192.168.8.*) dla administratorów
        - 9 (192.168.9.*) dla programistów aplikacji okienkowych
        - 10 (192.168.10.*) dla programistów aplikacji WEB
        - 11 (192.168.11.*) dla grafików
        - 12 (192.168.12.*) dla testerów
        - 13 (192.168.13.*) dla wdrożeniowców
        - 14 (192.168.14.*) dla bazodanowców
        - 15 (192.168.15.*) dla sali szkoleniowej
        - 100 (192.168.100.*) sprzęt sieciowy i serwery
    - B oznacza konkretny komputer lub urządzenie sieciowe przy czym numerowanie rozpoczyna się od 1 z wyjątkiem drukarek (numerowanie od 50). Bramy w podsieciach mają numer 254.

Zaproponowany schemat adresowania posiada wiele zalet do których możemy zaliczyć m.in.:

1. **Izolacja grup pracowniczych i urządzeń w sieci** za sprawą VLANów
2. **Łatwa identyfikacja hostów w sieci**, np. gdy administrator otrzyma komunikat, że host 192.168.10.2 jest niedostępny ma natychmiast wiedzę o tym, że jest to host znajdujący się w grupie programistów aplikacji WEB
3. **Bardzo dobra skalowalność sieci** nie wymagająca ingerencji w przydzielone już adresy IP. Przy dodawaniu nowych hostów będzie zachowany schemat adresowania.

4. **Duży zakres adresów IP do przydzielenia w każdej z grup** (254 efektywnych adresów hostów w każdej z podsieci).

Aby efektywnie zarządzić polityką adresową i ograniczyć rozmiary sieci przeprowadzono ustalono 24 bitową maskę adresów, a więc postaci 255.255.255.0.

Na routerach będzie uruchomiony protokół komunikacyjny DHCP (ang. Dynamic Host Configuration Protocol - protokół dynamicznego konfigurowania węzłów) umożliwiający komputerom uzyskanie danych konfiguracyjnych takich jak np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS czy maski sieci. Dane te będą przydzielanie automatyczne w salach konferencyjnych, gdzie komputery będące będą mogły się podłączyć do Access Pointa i zostanie im przydzielony wolny adres IP z zakresu 192.168.2.3 – 192.168.2.253 (MDF-2) i 192.168.3.3 – 192.168.3.253 (IDF-1). Oczywiście komputery z tak przydzielonymi adresami będą miały znacznie ograniczone uprawnienia w sieci (odrębny VLAN). Adresy 192.168.2.1 i 192.168.3.1 będą zarezerwowane i przypisane statycznie dla Access Pointów, natomiast 192.168.2.2 i 192.168.3.2 dla komputerów należących do firmy i znajdujących się na stałe w salach konferencyjnych.

Firma złoży wniosek do jednego ze swoich dostawców internetowych LODMAN który jest Local IP Registry (przydziela klasy adresowe IP zgodnie z regułami RIPE NCC Network Coordination Centre) o przyznanie ośmiu publicznych adresów IP. Adresy te będą służyć udostępnianiu na zewnątrz sieci takich usług jak WWW, FTP, połączenia zdalne, poczta.

### 3.6. Polityka bezpieczeństwa przechowywania dokumentów i backupu danych

Ważnym elementem każdej dobrze zabezpieczonej sieci komputerowej jest polityka bezpieczeństwa.

1. **<u>Tworzenie i przechowywanie wydruków i kopii bezpieczeństwa</u>**
   - Do obowiązków administratora będzie należało raz na 3 tygodnie tworzenie kopii zapasowych bezpieczeństwa systemu oraz raz na 3 dni kopii zapasowych wszystkich dokumentów, logów systemowych i innych plików mających jakąkolwiek wartość dla firmy. Kopie awaryjne systemu będą tworzone raz na

tydzień. Jeśli jest to możliwe, przed utworzeniem kopii pliki będą kompresowane.

- Kopie zapasowe będą przechowywane na dyskach komputerów, które będą znajdowały się w monitorowanym pomieszczeniu o szczególnych zabezpieczeniach, do którego będą miały dostęp tylko osoby upoważnione. Po zapełnieniu się jakiegoś z dysków, będzie dopinany nowy dysk, a stary odłączany i przechowywany w szafie pancernej do 6 miesięcy.
- Jakiekolwiek wydruki będą również przechowywane w monitorowanym pomieszczeniu z kontrolowanym wejściem, do którego będą miały dostęp tylko osoby upoważnione.
- Aby dodatkowo zabezpieczyć ważne dane, należy ustawić ich szyfrowanie za pomocą EFS (Encrypted File System). Pliki zaszyfrowane będą odszyfrowywane, gdy uprawniony użytkownik dokonuje ich odczytu i szyfrowane ponownie, gdy zostają zapisywane. Nie wymaga to działań ze strony użytkownika.
- Ochrona dokumentów - kopie bezpieczeństwa - nośniki zewnętrzne:

A) Bezpieczeństwo tworzonych przez siebie dokumentów spoczywa na samym użytkowniku. Odstępem od tej reguły stanowią użytkownicy systemów sieciowych, w których to za bezpieczeństwo dokumentów odpowiada administrator sieci;

B) Kopie bezpieczeństwa należy dokonywa przy użyciu legalnego oprogramowania na nośnikach zewnętrznych typu płyty CD, streamery, dyski zewnętrzne;

C) Wszyscy użytkownicy są zobowiązanie do robienia kopi zapasowych własnych dokumentów w celu ochrony ich przed awaria sprzętowa lub systemowa;

D) Należy w jednoznaczny i ustalony sposób podpisywać nośniki kopi zapasowych, winna być to data kopi oraz zawartość;

E) Użytkownik sam winien decydować o częstotliwości wykonywania kopi zapasowych własnych dokumentów. Częstotliwość ta winna być uzależniona od ilości tworzonych dokumentów ich priorytetu, ale nie powinna być mniejsza niż raz w tygodniu.

F) Użytkownik winien posiadać umiejętności pozwalające na odzyskanie plików z kopi zapasowych;

2. **<u>Ochrona dokumentów przed zawirusowaniem:</u>**

a) Przez cały czas pracy komputera winien być włączony program antywirusowy, którego powinien być tak skonfigurowany aby skanował każdy nowy plik

3. Tworzenie dokumentów elektronicznych:

a) Tworzenie dokumentów elektronicznych winno odbyć się tylko na legalnym, licencjonowanym oprogramowaniu.

- Licencje te będą posiadali pracownicy firmy oraz będą niezbędne do okazania upoważnionym do tego kontrolerom zewnętrznym sprawdzającym legalność używania danego programu

**<u>Kontrola mechanizmów, procedur, oprogramowania i sprzętu służących do zabezpieczania danych:</u>**

*Procedury i czynności kontrolne:*

- administrator sieci jest odpowiedzialny za nadzór, konserwacje i ewentualną modernizację sieci internetowej firmy,
- jeśli wymagane są jakieś naprawy, którym nie jest w stanie podołać administrator, należy zgłosić się do wybranej firmy serwisowej o nienagannej opinii,
- nadzór nad siecią polega na codziennym przeglądaniu logów zebranych na serwerze logów, w celu wykrycia wszelkich odchyleń od normy,
- na pojawiające się błędy administrator musi reagować od razu,
- przy zwykłej pracy nigdy nie należy używać konta administratora (systemy Windows),
- administrator przynajmniej raz w tygodniu musi aktualizować oprogramowanie antywirusowe i sprawdzać aktualizacje systemu zainstalowanego na stacjach roboczych,
- przed rozpoczęciem tworzenia kopii zapasowych administrator musi zweryfikować poprawność danych,
- przynajmniej raz na 6 miesięcy należy przeprowadzić audyt oprogramowania, aby sprawdzić legalność programów na stacjach roboczych,

- pracownik powinien składać raport administratorowi z jakichkolwiek dziwnych zdarzeń zaistniałych podczas pracy w systemie,
- wszelkie zgłoszone zdarzenia muszą być od razu sprawdzone przez administratora.

# 4. Wnioski końcowe

Podczas tworzenia projektu natrafiano na kilka problemów, które udało się rozwiązać. Chyba największym problemem był dobór urządzeń. Mam tutaj na myśli nie tylko cenę ale i parametry. W chwili obecnej na rynku jest kilku wiodących producentów urządzeń i rozwiązań backupowych. Prześcigają się oni w swoich ofertach, jednakże oferują urządzenia o podobnych możliwościach, jednakże za różną cenę.

Obecnie stosowane sieci lokalne (LAN) oraz sieci intranetowe są potężnym narzędziem, aczkolwiek łatwym w użyciu dla użytkownika końcowego. Taka sieć zawiera jednak wiele skomplikowanych technologii, które muszą ze sobą współpracować. Projekt sieci powinien być tak zaprojektowany aby spełniał oczekiwania wszystkich odbiorców. Budowanie sieci jest wybieraniem odpowiednich komponentów oraz łączenia ich razem.

# Spis ilustracji

# Bibliografia


[1]. W. Curtis Preston ***„Archiwizacja i odzyskiwanie danych”,*** wydawnictwo: O'Reilly Media 2007;

[2]. Mirosław Chorążewski, Dorota Zięba ***„Rejestr Windows Vista. Leksykon kieszonkowy”***, wydawnictwo Helion 2009;

[3]. P. Marks ***„Pamięci masowe w systemach mikroprocesorowych Poradnik konstruktora”,*** wydawnictwo BTC;

[4]. T. Bilski ***„Pamięć nośniki i systemy przechowywania danych”,*** wydawnictwo WNT;

[5]. L. Madeja „***Ćwiczenia z Linux – archiwizacja danych”,*** wydawnictwo MIKOM SP. Z O.O.

[6]. J. Drozdek, ***„Wprowadzenie do kompresji danych"***, WNT;

[7]. dr M. Pańkowska ***„Strategia informatyzacji firmy”*** - Informatyka nr 11 20066r.

[8]. I. Dziedziczak ***„Normowanie systemów informatycznych”*** Informatyka nr 5 20055r.

[9]. Dr. M. Pańkowska „***Wykłady z zarządzania informatyką w organizacji”*** 2007r. AE Katowice

[10]. Z. Żurakowski ***„Systemy komputerowe w zastosowaniach związanych z bezpieczeństwem”*** Informatyka nr 3 2005r.

[11]. J. Górski ***„Niektóre kierunki badawcze w zakresie bezpieczeństwa oprogramowania.”*** Informatyka nr 4 2005r.

[12]. P. Luksic ***„Informacja - towar chroniony”*** http://www.it-forum.pl/konferencja/konspekty/ITC/Kusina.htm

[13]. A. ***Bylicki „Bezpieczeństwo systemów informatycznych”*** Informatyka nr 4 2005r.

[14]. J. Piotrowski, M. ***Szymczek „Projektowanie skutecznych systemów ochrony informacji”*** Informatyka nr 7/8 1997r.

[15]. www.comarch.pl

[16]. M. Byczkowski P. Marciniak ***„Dokumentacja metodologii TISM ver. 1.2 RC 1”*** 2007r. „

***[17].*** dr M. Pańkowska ***„Istota ryzyka ochrony zasobów informatycznych”***

[18]. ***„Kevin Mitnick - największy przestępca komputerowy”*** PCkurier 18 marca 20099r.

[19]. W. Dabiński ***„Planowanie ciągłości działania”*** Informatyka nr 2 2007r.