**5. Różnice między wyszukiwaniem informacji a wyszukiwaniem danych.**

Różnice między wyszukiwaniem informacji, a wyszukiwaniem danych wynikają bezpośrednio z różnic między informacjami, a danymi.

Dane (ang. data) — to litery, słowa, teksty, liczby, znaki, symbole, kombinacje liter, liczb, symboli i znaków. Dane przetwarza się po to by otrzymać informację, wiadomość. Informacja jest produktem finalnym przetwarzania danych.

Istotną cechą danych jest brak uporządkowania; jest to zbiór nieuporządkowany. Ale jednocześnie dana jest wiarygodna i pewna (przy odpowiednim przechowywaniu). Dane w każdej chwili mogą być weryfikowane pod względem poprawności i aktualizowane. Dane pełnią także rolę nośników przepływu informacji.

Informacja jest zbiorem uporządkowanym wg określonego kryterium i poddanym interpretacji. Cechą każdej informacji (jako wyniku interpretacji) jest jej niepewność i ograniczona w czasie trwałość (wiarygodność). W popularnym pojmowaniu informacji zwracamy uwagę na ilość informacji (dużo, mało). Z informacją wiążemy także pojecie jakości, na którą składa się wierność przekazu, wiarygodność, szybkość i sposób archiwizowania.

Z powyższych rozważań wynika, że dane i informacje różnią się własnościami. Okazuje się, że z "morza danych" możemy uzyskać niewiele informacji i odwrotnie — z niewielkiej ilości danych można otrzymać znaczące informacje. Tak więc ilość informacji nie jest zależna do ilości danych.

Wyszukując dane szukamy surowych faktów, które trzeba dokładnie określić. Natomiast wyszukując informacje można się podpierać wyrazami bliskoznacznymi oraz kontekstem tego co chcemy znaleźć.

<http://ezinearticles.com/?What-is-the-Difference-Between-Data-Retrieval-and-Information-Retrieval?&id=3985949>

**6. Działanie systemu informacyjnego w sieci komputerowej.**

System informacyjny to zestaw współdziałających składników w celu gromadzenia, przetwarzania, przechowywania i udostępniania informacji, aby wspomagać podejmowanie decyzji, koordynowanie, sterowanie, analizowanie i wizualizację informacji.

System informacyjny, w którym procesy przetwarzania danych i procesy komunikacyjne realizowane są technikami tradycyjnymi nazywamy tradycyjnym systemem informacyjnym, o systemie z zastosowaniem technik komputerowych mówimy, że to system informatyczny.

Obecnie ważniejsze jest dotarcie do informacji niż jej gromadzenie, użytkownik ma możliwość bezpośredniego dostępu do informacji bez instytucji pośredniczących. Czas i przestrzeń dzięki połączeniom sieciowym nie odgrywają już takiej roli, jak niegdyś. Ważna jest także sprawa aktualności danych. W przypadku dokumentów drukowanych istnieje niebezpieczeństwo ich dezaktualizacji już w momencie opublikowania. Dokumenty elektroniczne w sieciach dostępne są w trybie czasu rzeczywistego. Poza tym istnieje możliwość aktualizowania danych na bieżąco.

System informacyjny w sieci taki jak sieciowa baza danych, czy jakiś system składowania informacji. Wyszukiwanie w Google jako w sieciowym, rozproszonym systemie informacyjnym.

Coraz bardziej złożone aplikacje WWW.

System biblioteki PWr.

Gopher jest protokołem klient-serwer pozwalającym na rozpowszechnianie informacji w powszechnych/kampusowych systemach informacyjnych. Był pierwszym rozpowszechnionym systemem informacyjnym w sieci integrującym różne protokoły: FTP, telnet, WAIS własne struktury danych z możliwością dostępu do różnych typów danych, tak czysto tekstowych, jak i grafik i danych czysto binarnych (archiwów wszelkiego rodzaju). Został później wyparty przez WWW z powodu sztywnej, hierarchicznej struktury (gdzie jednym z elementów ścieżki dostępu był typ pliku), niewygodnych metod tworzenia serwisów, braku pełnej "multimedialności" oraz dlatego, że WWW zyskał większe wsparcie tak producentów jak i środowisk akademickich.

WWW jest zbiorem powiązanych ze sobą zasobów i dokumentów, połączonych hiperłączami i URL-ami. Krótko mówiąc, Web jest aplikacją działającą w Internecie. Przeglądanie stron internetowych WWW zwykle rozpoczyna się albo od wpisania adresu strony w przeglądarce internetowej, albo poprzez podanie linku do tej strony lub linku do konkretnego zasobu. Następnie przeglądarka wysyła do serwera WWW, na którym zlokalizowana jest strona, szereg niewidzialnych dla nas zapytań, aby później pobrać zawartość danej strony i wyświetlić ją na ekranie monitora.

**7. Technologie multimedialne stosowane w systemach informacyjnych.**

·         WWW

·         HTML5

·         Flash

·         VoD

·         Gry sieciowe

·         Telekonferencje (przesyłanie, strumieniowanie obrazu, dźwięku, tekstu i innych danych)

**8. Efektywność systemów informacyjnych.**

Efektywność opisuje stopień wykorzystania zasobów sprzętowych i programowych stanowiących  podstawę działania systemu informacyjnego.

Zła organizacja i niska efektywność systemu skutkują wzrostem kosztów działalności organizacji,, spadkiem jakości obsługi, utrudnionym dostępem do informacji na różnych szczeblach, ich znaczną niekompletnością, wydłużonym czasem generowania.

Jedną ze strategii zwiększenia efektywności pracy zespołów projektujących systemy informacyjne jest wielokrotne używanie raz opracowanych fragmentów projektu lub modułów programowych. Ponowne użycie wcześniej opracowanego fragmentu projektu albo modułu programu ma wiele zalet, wśród których na plan pierwszy wysuwają się: obniżenie kosztów, przyspieszenie realizacji projektu oraz minimalizacja błędów.

Na efektywność systemu informacyjnego ma wpływ wiele czynników: poziom wyszkolenia pracowników, zastosowane oprogramowanie, infrastruktura sprzętowa, rozwiązania sieciowe, dostosowanie systemu do wielkości firmy oraz prognozowanego wzrostu. Często okazuje się, że w miarę rozwoju firmy, przestają sprawdzać się - uprzednio wystarczające - rozwiązania.

**9. Zadania projektowania sieci komputerowej.**

Warunki, które powinien spełniać dobry projekt sieci komputerowej:

·         Realizacja oczekiwań zleceniodawcy

·         Fachowa dokumentacja

·         Możliwość rekonfiguracji i rozbudowy sieci

·         Łatwość rekonfiguracji w przypadku awarii

·         Niezależność uszkodzeń w różnych segmentach sieci

·         Bezpieczeństwo danych i serwerów.

Zasady:

·         Nie wolno osiągać granic możliwości sieci/sprzętu.

·         Maksymalna długość kabla dla 5 kategorii: 3m do komputera, 90m kabla poziomego, 6m kabla krosującego.

·         Maksymalne promienie zagięcia: 4 x średnica kabla.

·         Zgodnie z ISO: 10 metrów kwadratowych na miejsce pracy (nie oznacza to 1 gniazdka na 10m2, ale co najmniej 1 gniazdko na 10m2).

·         Każda kondygnacja musi być wyposażona w minimum 1 punkt dystrybucyjny. W przypadku pomieszczeń o powierzchni większej od 1000m2 lub w przypadku, kiedy okablowanie poziome przekracza 90 m należy wprowadzić dodatkowy punkt dystrybucyjny.

·         Określona powierzchnia punktu dystrybucyjnego w zależności od obsługiwanej powierzchni.

·         Maksymalna dozwolona ścieżka sygnału obejmuje 5 segmentów kabla połączonych 4 hubami. W takim przypadku 2 z tych segmentów mogą być użyte wyłącznie jako połączenia między hubami. Jeśli się nie da inaczej, należy podzielić sieć na domeny kolizyjne (podsieci) i wprowadzić switche.

·         Maksymalnie 1024 urządzenia na podsieć.

·         Maksymalna całkowita odległość w podsieci 500m.

Projektowanie:

·         Przeanalizować wymagania klienta i określić wymagania projektowe.

·         Opracować schemat logiczny sieci.

·         Określić potrzebne urządzenia (panele krosownicze, switche, routery, AP), a także kable, listwy, końcówki.

·         Odpowiednio poprowadzić kable (pionowo i poziomo), wykorzystując infrastrukturę (łatwy dostęp, minimalizowanie uszkodzeń, oznakować kable).

·         Określenie podłączenia do Internetu.

·         Ustawienie punktu dystrybucyjnego.

·         Serwer i jego zadania.

·         Ustalić adresację.

·         Ew. zabezpieczyć sieć.

·         Sporządzić kosztorys.

**10. Klasyfikacja ruchu teleinformatycznego.**

Klasyfikacja ruchu jest automatycznym procesem, który kategoryzuje ruch sieciowy ze względu na różne parametry, takie jak numer portu, protokół czy wielkość pakietu. Każda z klas ruchu może być traktowana inaczej i przesyłana z innym priorytetem. Najlepszym przykładem jest priorytetyzacja ruchu VoIP, tak aby użytkownicy na obu końcach nie odczuwali zakłóceń.

Typowe klasy ruchu:

·         Sensitive traffic (ruch wrażliwy), np.: VoIP, gry sieciowe, telekonferencje, przeglądanie sieci

·         Best-effort traffic (ruch niegwarantowany), każdy inny np.: ruch e-mailowy, P2P

·         Undesired traffic (ruch niepożądany), np.: SPAM, robaki, botnety

·         W DiffServ pakiety są klasyfikowane do kilku klas usług (zagregowanych strumieni ruchu).

·         W IntServ zakłada się, że zasoby w sieci są rezerwowane dla pojedynczych strumieni danych.

·         Usługa Best effort transmituje dane w sieci o możliwie najwyższej przepustowości ale za to bez gwarancji poziomu usług.

**11. Zarządzanie zasobami sieci komputerowej.**

Typy sieci ze względu na zarządzanie zasobami:

·         Sieci równorzędne (każdy-z-każdym) P2P (od ang. peer-to-peer – równy z równym) – model komunikacji w sieci komputerowej, który gwarantuje obydwu stronom równorzędne prawa (w przeciwieństwie do modelu klient-serwer). W sieciach P2P każdy komputer może jednocześnie pełnić zarówno funkcję klienta, jak i serwera. Każdy węzeł sieci (czyli komputer użytkownika) odgrywa rolę serwera przyjmując połączenia od innych użytkowników danej sieci, jak i klienta, łącząc się i pobierając dane z innych maszyn działających w tej samej sieci. Wymiana danych jest zawsze prowadzona bez pośrednictwa centralnego serwera.

·         Sieci oparte na serwerach (klient-serwer) - w sieciach klient-serwer zasoby często udostępniane gromadzone są w komputerach odrębnej warstwy, zwanych serwerami. Serwery zwykle nie mają użytkowników bezpośrednich. Są one raczej komputerami wielodostępnymi, które regulują udostępnianie swoich zasobów szerokiej rzeszy klientów. W sieciach tego typu zdjęty jest z klientów ciężar funkcjonowania jako serwery wobec innych klientów.

·         P2M

·         Dropbox

Zasoby:

·         Plikowe na serwerach i hostach.

·         Serwery FTP, wydruku, dhcp, dns, itp.

·         Procesory, pamięć masowa i ich użycie, zarówno na serwerach jak i na stacjach roboczych.

·         Połączenia sieciowe, przepustowość łącz.

·         Switche, routery i inne urządzenia sieciowe.

·         Ludzie, administratorzy, zarządzanie nimi oraz ich uprawnieniami.

·         Backup danych.

·         Zarządzanie systemem pocztowym.

·         Zarządzanie bezpieczeństwem (firewalle, antywirusy).

Narzędzia pozwalające na równoważenie obciążenia w środowisku heterogenicznym systemów komputerowych: algorytmy rozdziału zasobów, języki i sposoby (narzędzia) specyfikacji zasobów, mapowanie zasobów do aplikacji.

**12. Metody naprawiania błędów w systemach teleinformatycznych.**

Kodowanie korekcyjne lub kodowanie korygujące (ang. ECC - error correction coding, FEC - forward error correction) – technika dodawania nadmiarowości do transmitowanych cyfrowo informacji. Umożliwia całkowitą lub częściową detekcję i korekcję błędów powstałych w wyniku zakłóceń. Dzięki temu nie ma potrzeby wykorzystywania kanału zwrotnego, do poinformowania nadawcy o błędzie i konieczności ponownego przesłania informacji. Kodowanie korekcyjne jest więc wykorzystywane wtedy, gdy retransmisja jest kosztowna, kłopotliwa lub niemożliwa, np. ze względu na ograniczenia czasowe. Przykłady:

·         Kod splotowy

·         Kod Hamminga

·         Kodowanie korekcyjne Reeda-Solomona

·         Kod cykliczny

·         Kod BCH

·         Potrójne przesyłanie danych

Powszechnie stosowaną korekcją jest sekwencja BCC (Block Check Character) przedstawiająca znak lub sekwencję znaków generowaną przez algorytm kontrolny przed wysłaniem wiadomości w łącze transmisji danych. Urządzenie odbiorcze porównuje odtworzoną sekwencję kontrolną z sekwencją odebraną, aby stwierdzić, czy wystąpiły błędy transmisji. Wykorzystuje się przy tym następujące metody protekcji:

·         pionowe sprawdzenie danych VRC (Vertical Redundancy Checking), polegające na generowaniu bitu parzystości dla każdego znaku;

·         wzdłużną kontrolę danych LRC (Longitudinal Redundancy Checking), polegającą na obliczeniu parzystości dla kolejnych bitów: pierwszego, drugiego itd. — we wszystkich znakach w przesyłanym bloku. Kontrolę LRC łączy się często z VRC;

·         cykliczną kontrolę danych CRC (Cyclic Redundancy Checking).

Przy protekcji CRC blok informacyjny traktuje się jako wielomian, który w nadajniku dzieli się modulo 2 przez wielomian CRC, zwykle szesnastego stopnia (CCITT zaleca kilka, popularnym jest x16+x12+x5+1). Otrzymana reszta tworzy 16-bitową sekwencję kontrolną FCS (Frame Check Sequence) transmitowaną na końcu bloku. W odbiorniku odebrany blok informacyjny również dzieli się przez taki sam wielomian. Przez porównanie otrzymanej reszty z dzielenia z odebraną sekwencją kontrolną można stwierdzić wystąpienie błędu transmisji. Brak zgodności sekwencji wymusza przesłanie odpowiedniej informacji kanałem sprzężenia powrotnego i retransmisję błędnych bloków.

Retransmisja ramek.

**13. Koncepcje dostarczania jakości usług w sieciach teleinformatycznych.**

·         kształtowanie i ograniczanie przepustowości

·         zapewnienie sprawiedliwego dostępu do zasobów

·         nadawanie odpowiednich priorytetów poszczególnym pakietom wędrującym przez sieć

·         zarządzanie opóźnieniami w przesyłaniu danych

·         zarządzanie buforowaniem nadmiarowych pakietów: DRR, WFQ, WRR

·         określenie charakterystyki gubienia pakietów

·         unikanie przeciążeń: Connection Admission Control (CAC),

Parametry QoS:

·         przepustowość

·         straty pakietów

·         opóźnienia

·         zmienność opóźnienia (jitter)

Algorytmy kolejkowania:

·         FIFO

·         Algorytm karuzelowy (round-robin) - Algorytm karuzelowy (Round-robin) mówi, że można stworzyć tyle kolejek ile jest strumieni oraz zdejmować pakiety po jednym z każdego pasma w stałym porządku. Jeśli dane pasmo nie ma nic do wysłania, przechodzi się do kolejnego bez tracenia czasu. W ten sposób, jeśli połączenie zaczyna wysylać dane, ma pewność, że pierwszy pakiet zostanie wysłany nie później niż po czasie jednego okresu. Dzieli pakietowo.

·         Priorytetowe (PQ) – tworzone są kolejki o różnych priorytetach. Do każdego przybywającego pakietu przypisuje się odpowiednią klasę priorytetu. Klasa priorytetu może być zależna od szeregu czynników np. źródłowego adresu IP, wartości bitów Type of Service, numeru portu, interfejsu wejściowego, protokołu, itp. Kolejka o niższym priorytecie obsługiwana jest dopiero, gdy kolejka o wyższym priorytecie będzie całkowicie opróżniona. Oznacza to, że jeśli jest dużo pakietów o wysokim priorytecie może dojść do dużych opóźnień w kolejkach o najniższych priorytetach. Pakiety należące do tej samej klasy priorytetu obsługiwane są metodą FIFO.

·         Sprawiedliwe (SFQ) - Dane przepływające przez interfejs są dzielone na strumienie, które są przydzielane do odpowiadających im kolejek FIFO. Kolejki są kolejno opróżniane tak aby żadna z nich nie mogła wykorzystać całej przepływności łącza. Przy dużej liczbie strumieni, do jednej kolejki może być przydzielone więcej niż jeden strumień. Co pewien czas przydział strumieni do kolejek jest zmieniany za pomocą odpowiedniego algorytmu mieszającego. Dzieli bitowo.

·         Ważone sprawiedliwe (WFQ) - analizuje nagłówek IP i odczytuje wartość priorytetu. Następnie przydziela proporcjonalnie więcej pasma transmisjom z wyższym priorytetem. Powoduje to, że w pierwszej kolejności obsługuje ruch o najwyższym priorytecie, przykładowo związany z aplikacjami strumieniowymi, a dopiero w dalszej pozostałe pasmo jest sprawiedliwie dzielone między innymi aplikacjami.

·         RED (Random Early Detection) - Wykorzystywany jest w sytuacjach ciągłego, długotrwałego przeciążenia węzłów w sieci. Mechanizm RED, tuż przed wystąpienie zatoru, rozpoczyna losowe odrzucanie pakietów w celu zmniejszenia ruchu generowanego przez niektóre źródła. Rozwiązanie takie pozwala na lepsze wykorzystanie pasma oraz zapobiega wystąpieniu globalnej synchronizacji. Działanie mechanizmu RED opiera się na wyznaczeniu średniej długości kolejki i przyrównywaniu jej zajętości do dolnego i górnego progu (rys. 3.7). W sytuacji, gdy średni rozmiar kolejki znajduje się poniżej minimalnego progu, to żadne pakiety nie są odrzucane. Wypełnienie kolejki na poziomie między minimalnym i maksymalnym progiem powoduje losowe odrzucanie pakietów z odpowiednim prawdopodobieństwem. Czym bardziej kolejka jest zajęta, tym więcej odrzucanych jest pakietów. Przekroczenie górnej granicy skutkuje odrzucaniem wszystkich pakietów. Konsekwencją takiego działania jest większe prawdopodobieństwo odrzucania pakietów ze źródeł generujących większy ruch.

Profilowanie ruchu:

·         Leaky Bucket - Parametrami algorytmu są: wielkość bufora – „wiadra” – oraz liczba danych jakie opuszczają bufor w jednostce czasu podana w bajtach lub bitach na sekundę. Algorytm ten umożliwia dokładne określenie z jaką częstością dane będą pobierane z kolejek i przesyłane przez sieć. Podstawę działania „cieknącego wiadra” stanowi pojedynczy bufor – kolejka FIFO gromadząca pakiety. Posiada określoną maksymalną długość. Dodatkowo należy wspomnieć, że pewne pakiety wchodzące do bufora mogą zostać odrzucane na skutek ich przedawnienia lub przekroczenia rozmiaru samej kolejki. Wówczas takie nadmiarowe pakiety muszą zostać odrzucone. Jednak zyskiwana jest pewność, że łącze, w którym zastosowano kształtowanie ruchu nie będzie przeciążone. Wadą tego algorytmu jest to, że nie pozwala on na chwilowe wzrosty natężenia ruchu zaraz po jego rozpoczęciu.

·         Token Bucket - do wiadra wpadają żetony w stałym tempie (odpowiednik   z wersji cieknącej). Kiedy wiadro się zapełni, napływające żetony są odrzucane. Każdy żeton reprezentuje pozwolenie na wysłanie określonej ilości bitów. Aby wysłać pakiet, wymagana jest ilość żetonów odpowiadająca bitowo wielkości pakietu. Po wysłaniu pakietu ,,wykorzystane'' żetony są usuwane z wiadra. Jeśli brak jest wystarczającej ilości żetonów – pakiet, w zależności od implementacji, czeka, jest zaznaczany lub odrzucany. Żetony odrzucone ze względu na przepełenie wiadra nie mogą już być wykorzystane do wysyłania pakietów. Zatem maksymalna możliwa fala wysyłanych pakietów jest proporcjonalna do wielkości wiadra.  Głównym atutem w porównaniu z cieknącym wiadrem jest możliwość chwilowego wysłania większej ilości danych jeśli bezpośrednio wczesniej przepustowość wiadra nie była wykorzystywana w pełni. Innymi słowy, przez pewien czas (zależny od wielkości wiadra oraz jego zapełniena żetonami) pakiety mogą być wysyłane bez ograniczeń.

·         Hierarchical Token Bucket - algorytm hierarchicznego podziału łącza. Umożliwia on: podział pasma na klasy; przyporządkowanie różnego rodzaju pakietów IP do odpowiednich klas według różnych kryteriów, na przykład według adresu odbiorcy, adresu nadawcy, wielkości pakietu, protokołu itp.; nałożenie reguł i ograniczeń na przepływność dla poszczególnych klas; dzielenie hierarchiczne, tj. każda klasa może być podzielona na wiele podklas. Największą zaletą jest fakt,  że można pozwolić na podział łącza najpierw według odbiorców, czy nadawców, a następnie w ramach ich wyodrębnionego ruchu jeszcze podział na konkretne usługi.

·         Class Based Queueing, CBQ – algorytm kolejkowania pakietów oparty na klasach kolejek. Umożliwia wydzielanie pasma dla komputerów w sieci lokalnej, tak aby każda ustalona klasa pakietów miała zagwarantowaną szerokość pasma.