INFORMATYKA

Notatki

ZESPÓŁ SZÓŁ PUBLICZNYCH w POLANOWIE

Temat 1: Zasady zgodnego z prawem wykorzystania komputera.

Rodzaje licencji oprogramowania

1. **Freeware** – są całkiem za darmo nie posiadają ograniczeń.
2. **Shareware** – programy za darmo umożliwiające sprawdzenie danego programu, jeśli program się podoba klientowi może kupić wersję komercyjną. Programy tego typu posiadają pewne ograniczenia np.:
   - Ograniczenie ilości uruchomień, np. po 40 uruchomieniach programu nie można już uruchomić.
   - Ograniczenie czasowe np. program uruchamia się przez 30 dni.
   - Ograniczenie funkcji programu – np. w programie graficznym nie można zapisać pliku.
3. **Trial** – Programy na tej licencji są w pełni funkcjonalne. Licencja pozwala używać program przez z góry ustalony czas (np. 90 dni). Po upływie tego czasu, jedyną rzeczą, na którą pozwoli program to rejestracja albo usunięcie z dysku twardego.
4. **Demo** – wersja demonstracyjna - wersja o ograniczonej funkcjonalności w stosunku do wersji pełnej. W przypadku gier jest to zwykle jeden poziom z finalnej części gry. Dema są zazwyczaj wydawane przez wydawcę danej gry w celu zapoznania konsumentów z grą, aby mogli zdecydować o jej zakupie. Dema często wydawane są na płytach dołączanych do czasopism tematycznych.
5. **Open Source** (GNU/GPL) – oprogramowanie bezpłatne dające możliwość jego dalszego rozpowszechniania i modyfikacji oraz dostępności do jego kodu źródłowego.

Korzyści i ograniczenia wynikające z korzystania z legalnego oprogramowania

1. **Ograniczenia:**
   - Ograniczenie liczby kopii używanego programu (zwykle licencja określa ile kopii możemy używać).
   - Zakaz udostępniania programu innym użytkownikom.
2. **Korzyści:**
   - Upgrade – prawo do zniżkowego zakupu nowych wersji programu.
   - Bezpłatne porady (pomoc techniczna).
   - Serwis pogwarancyjny.
   - Support producenta (łatki, poprawki, darmowe nowsze wersje).
   - Brak wirusów, trojanów itp.
   - Szybszy rozwój IT (Technologii Informatycznej).

Netykieta

Netykieta – zbiór zasad przyzwoitego zachowania w Internecie, swoista etykieta obowiązująca w sieci (ang. net).

Netykieta, podobnie jak zwykłe zasady przyzwoitego zachowania, nie jest dokładnie skodyfikowana, nikt też nie zajmuje się systematycznym karaniem osób łamiących te zasady, jednak uparte łamanie zasad netykiety może się wiązać z różnymi przykrymi konsekwencjami, jak np.: zgłoszenie nadużycia i odcięcie „niegrzecznego” osobnika od określonej usługi internetowej przez jej administratora.

Zasady netykiety wynikają wprost z ogólnych zasad przyzwoitości lub są odzwierciedleniem niemożliwych do ujęcia w standardy ograniczeń technicznych wynikających z natury danej usługi Internetu.

Zalecenia netykiety

Grupy, listy dyskusyjne, poczta elektroniczna (e-mail):

- zakaz spamowania (m.in. wysyłania niechcianych linków do stron),
- zakaz wysyłania tzw. „łańcuszków szczęścia”,
- zakaz wysyłania e-maili do wielu osób naraz z jawnymi adresami poczty elektronicznej (stosujemy kopię ukrytą).

Komunikatory, czaty, fora dyskusyjne, na stronach WWW:

- zakaz floodowania (ang. flood),
- zakaz nagabywania (upartego łączenia się z) osób które sobie tego nie życzą,
- zakaz ciągłego pisania wielkimi literami.

Przykłady zachowań sprzecznych z netykietą:

- kłótnia internetowa,
- trollowanie.

Praca domowa

Sporządzić krótkie definicje wyrażeń:

- **floodowanie** (ang. flood),
- **trollowanie** (ang. trolling),
- **Prawo Godwina**,
- **plonk**,
- **lamer**.

Ograniczenia prawne

Treści, za które określono sankcje w kodeksie karnym, a które:

- namawiają do popełnienia lub doradzają w popełnieniu samobójstwa lub samookaleczenia

- grożą innym osobom popełnieniem przestępstwa na jego szkodę lub szkodę osoby jego najbliższej
- obrażają inne narodowości, rasy ludzkie, religie
- nawołują do popełnienia przestępstwa
- propagują totalitarny ustrój państwa lub nawołuje do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość

Treści, za które określono sankcje w kodeksie cywilnym, a które:

- lżą osoby publiczne,
- zawierają pomówienia – informacje obarczające niepotwierdzonymi zarzutami inne osoby,
- obrażają inne narodowości, rasy ludzkie, religie.

Treści, za które określono sankcje w ustawach szczególnych, a które:

- promują alkohol,
- przyczyniają się do łamania praw autorskich lub naruszają prawa autorskie i licencje,
- promują środki odurzające, narkotyki,
- ujawniają bez czyjejś wyraźnej zgody dane osobowe, identyfikatory komunikatorów internetowych, fotografie, adres poczty elektronicznej, miejsce zamieszkania, pracy, przebywania, numery telefonów, tablic rejestracyjnych i inne poufne dane,
- zawierają słowa powszechnie uznane za niecenzuralne.

Temat 2: Elementy zestawu komputerowego.

Definicja komputera

Komputer – to urządzenie elektroniczne służące do gromadzenia, przetwarzania i przechowywania danych w postaci cyfrowej.

Podstawowe części składowe zestawu komputerowego:

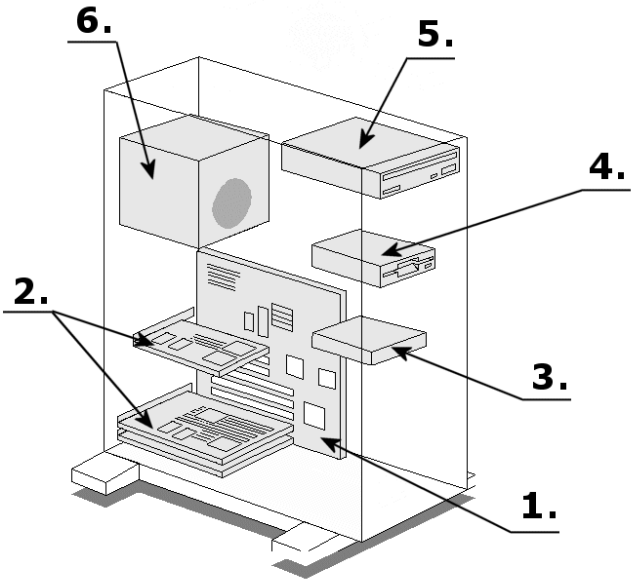
- **Jednostka centralna**
- **Monitor** – informacje wyświetlane na ekranie pochodzą z karty graficznej, która przekształca dane otrzymane z mikroprocesora. Tradycyjne monitory z lampami kineskopowymi określa się jako monitory CRT. Obecnie częściej można spotkać monitory ciekłokrystaliczne LCD.
- **Klawiatura** – to podstawowe urządzenie do wprowadzania danych. Standardowa klawiatura ma 101 klawiszy i kształt prostokąta.
- **Mysz** – w podstawie myszy znajduje się dioda oraz system czujników optycznych. Czujniki optyczne są źródłem danych generowanych podczas poruszania myszą. Działanie myszy polega na tym, że przesuwanie jej po podłożu powoduje przesyłanie impulsów elektrycznych do systemu. Tu napływające sygnały są odpowiednio interpretowane. W efekcie powoduje to ruch wskaźnika myszy na ekranie.

Urządzenia peryferyjne:

- **Skaner** – umożliwia przetworzenie obrazu (zdjęcie, tekst) na postać cyfrową i wprowadzenie go do pamięci komputera. W przypadku zastosowania programów do optycznego rozpoznawania znaków (tzw. OCR) można zeskanowany tekst zapisać jako dokument tekstowy, a następnie go edytować.

- **Mikrofon** – wykorzystanie mikrofonu jest możliwe pod warunkiem, że w jednostce centralnej zainstalowano kartę dźwiękową.
- **Głośniki i słuchawki** – wykorzystanie głośników czy słuchawek jest możliwe pod warunkiem, że w jednostce centralnej zainstalowano kartę dźwiękową.
- **Drukarka** – umożliwia utrwalenie wyników pracy swojej i komputera na papierze.
- **Kamera cyfrowa.**

Temat 3: Wewnętrzna budowa jednostki centralnej



1 – płyta główna
2 – karty rozszerzeń
3 – dysk twardy
4 – stacja dyskietek
5 – napęd CD-ROM lub DVD-ROM
6 – zasilacz

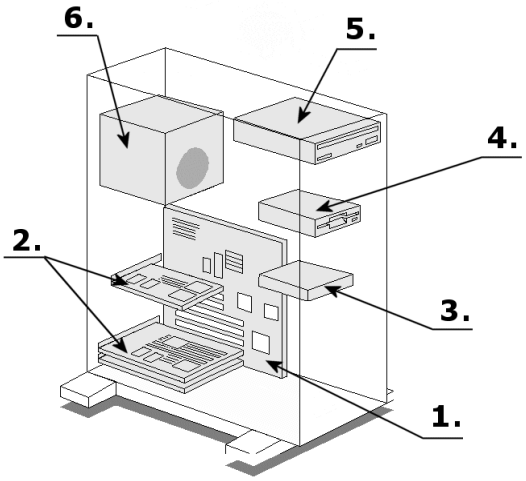
Płyta główna – jest jednym z najważniejszych elementów wewnętrznych komputera. Wyposażona w zamontowane na stałe układy i gniazda, w których można osadzić takie elementy jak mikroprocesor, pamięci lub karty rozszerzeń (graficzne, dźwiękowe, sieciowe). Do płyty głównej podłącza się napędy CD-ROM, DVD-ROM, stacje dyskietek czy dyski twarde. Istotnym elementem jest magistrala zapewniająca możliwość przepływu danych – czyli komunikowania się poszczególnych podzespołów. Najważniejszym układem płyty głównej jest **Chipset**, którego zadaniem jest nadzorowanie przepływu danych pomiędzy urządzeniami podłączonymi do magistrali.

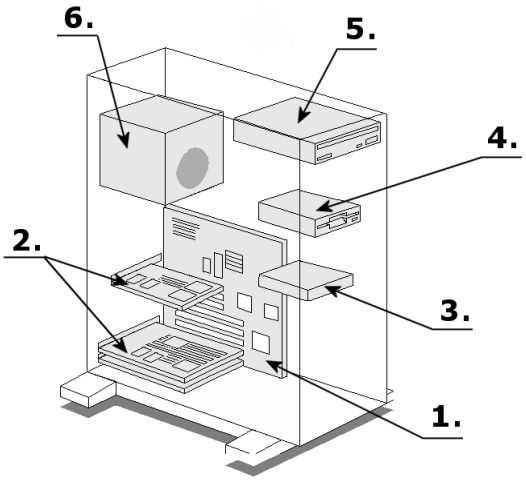
Mikroprocesor (procesor) – steruje pracą komputera. Jest to złożony element elektroniczny, zdolny do wykonywania operacji arytmetyczno-logicznych (np. dodawania) według dostarczonych mu instrukcji. Procesory podczas pracy wydzielają duże ilości ciepła, dlatego muszą być chłodzone. Radiator pozwala odprowadzić ciepło. Na radiatorze montuje się wentylator wspomagający chłodzenie.

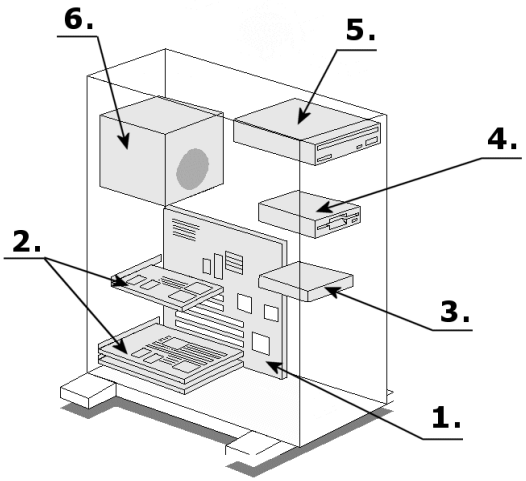
Karty rozszerzeń – na płycie głównej znajdują się gniazda PCI (białego koloru), służące do instalacji kart rozszerzeń umożliwiających rozbudowę komputera.

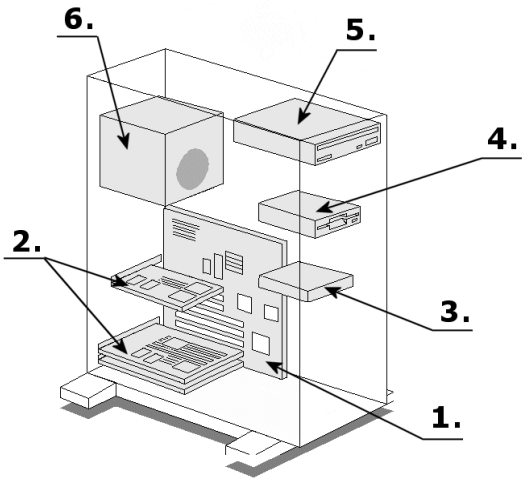
- **Modem wewnętrzny** – przetwarza, wysyła i odbiera dane między komputerami z użyciem standardowej linii telefonicznej.
- **Karta graficzna** – jest odpowiedzialna za wyświetlanie i jakość obrazu na monitorze.
- **Karta dźwiękowa** – generuje efekty dźwiękowe.
- **Karta sieciowa** – służy do łączenia komputerów ze sobą celem wymiany danych.
- **Karta telewizyjna** – umożliwia komputerowi pełnienie funkcji telewizora.

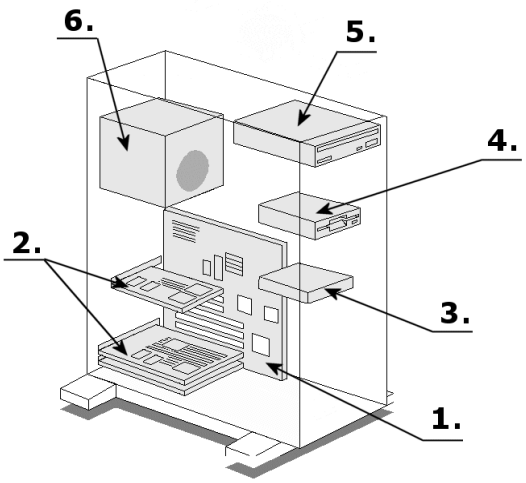
W jednostce centralnej montowane są również napędy CD-ROM, DVD-ROM, dysk twardy, (dawniej) stacja dyskietek oraz zasilacz.

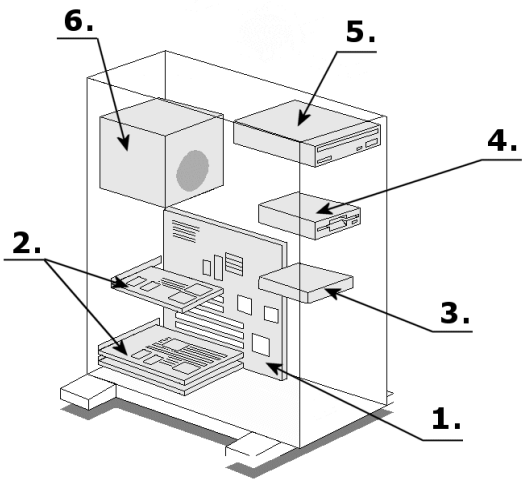

6.
5.
4.
2.
3.
1.


6.
5.
4.
2.
3.
1.


6.
5.
4.
2.
3.
1.


6.
5.
4.
2.
3.
1.

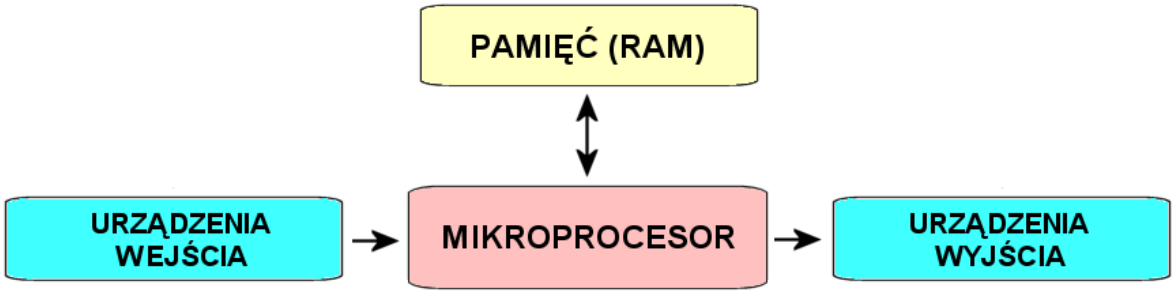

6.
5.
4.
2.
3.
1.


6.
5.
4.
2.
3.
1.

Temat 4: Urządzenia wejścia-wyjścia.

Ogólna budowa i zasada działania komputera

(schemat uproszczony)



Urządzenia wejścia (danych)

- Mysz komputerowa
- Klawiatura
- Kamera cyfrowa
- Skaner
- Mikrofon

Urządzenia wyjścia (danych)

- Monitor / Projektor multimedialny
- Karta grafiki
- Drukarka
- Głośniki i słuchawki

Temat 5: Rodzaje pamięci.

Jednostki informacji

1 bit (b) – najmniejsza jednostka informacji

8 b = 1 B (b – bit, B – bajt)

1024 B = 1 kB (kilobajt)

1024 kB = 1 MB (megabajt)

1024 MB = 1 GB (gigabajt)

1024 GB = 1 TB (terabajt)*

1024 TB = 1 PB (petabajt)

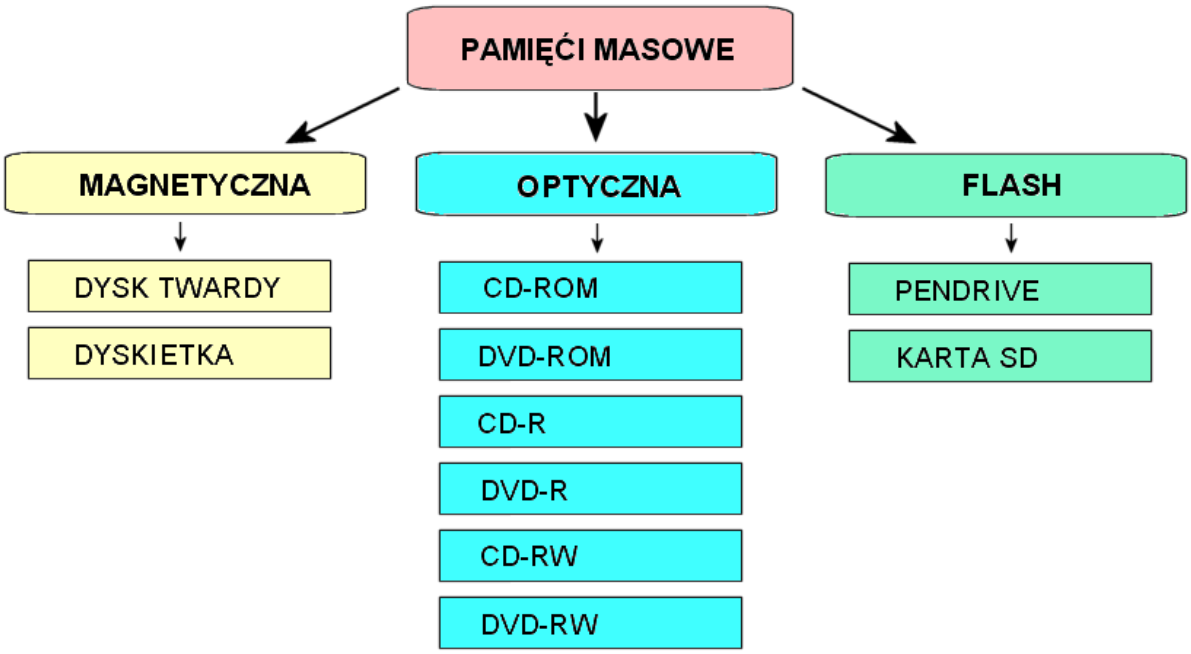
1024 PB = 1 EB (eksabajt)

* odtworzenie filmów znajdujących się na płytach DVD o łącznej pojemności jednego terabajta zajęłoby około 18 dób.

Pamięć wewnętrzna komputera

- **Pamięć RAM** (Random Access Memory) – pamięć o dostępie swobodnym, której komputery używają jako pamięci operacyjnej. Służy do zapisu i odczytu informacji. Mikroprocesor przechowuje tu dane operacyjne, powstające podczas pracy komputera. Pamięć ta jest nietrwała i dlatego dane są tracone po wyłączeniu komputera.
- **Pamięć ROM** (Read Only Memory) – to pamięć zaprogramowana fabrycznie i może być tylko odczytywana. Nie traci swojej zawartości po utracie zasilania. Pamięć (BIOS) ta umożliwia rozpoczęcie pracy komputera, rozruch poszczególnych podzespołów i współpracę mikroprocesora z pozostałymi częściami zestawu komputerowego.

Pamięci masowe



Pamięć magnetyczna

Wszystkie typy pamięci na warstwach magnetycznych działają na tej samej zasadzie; na poruszającej się warstwie magnetycznej dokonywany jest zapis informacji polegający na odpowiednim namagnesowaniu pól nośnika informacji.

Zapis i odczyt dokonywany jest za pomocą głowic. Głowicą nazywamy rdzeń z nawiniętą na nią cewką i niewielką szczeliną między biegunami. Zapis informacji sprowadza się do namagnesowania poruszającego się nośnika. Pole magnetyczne wytworzone w szczelinie magnesuje nośnik tak długo, jak długo płynie prąd w cewce głowicy. Namagnesowany odcinek nośnika zachowuje się jak zwykły magnes, wytwarzając własne pole magnetyczne.

Pamięć optyczna

Pamięć optyczna jest najczęściej spotykana pod postacią dysku wymiennego, w którym używa się materiałów zmieniających jaskrawość pod wpływem światła laserowego lub powoduje mechaniczne zmiany powierzchni nośnika. Powstające plamki, grudki lub otwory reprezentują bity.

Rodzaje nośników pamięci magnetycznych

1. Dysk twardy (ang. HDD – Hard Disk Drive) to urządzenie hermetycznie zamknięte, składający się od 1 do 8 wirujących talerzy pokrytych bardzo cienką warstwą magnetyczną, każdy talerz posiada osobną głowicę odczytująco-zapisującą. Dysk twardy jest zwykle na stałe włączony w skład jednostki centralnej i przechowuje dane, które powinny być zawsze dostępne – takie jak system operacyjny. Nowoczesne dyski twarde posiadają bardzo dużą przepustowość danych, niski czas dostępu do danych, obracają się z prędkością kilku lub kilkunastu tysięcy obrotów na minutę, a ich pojemność wynosi nawet kilka terabajtów.

2. Dyskietka (ang. FD - Floppy Disk) Dyskietka jest to krążek wykonany z giętkiego tworzywa sztucznego, pokryty warstwą materiału magnetycznego. Dysk o średnicy 3,5 cala ma pojemność 1,44 MB.

Rodzaje nośników pamięci optycznych

1. **CD-ROM** o standardowej średnicy 120 mm, są tłoczone w specjalnych prasach i mogą być tylko odczytywane. Istotną cechą tych płyt jest fakt, że służą wyłącznie do odczytu i nie można na nich zapisywać danych tak jak na dysku twardym gdzie można usuwać i tworzyć nowe dane. Pojemność płyty typu CD-ROM wynosi ok. 650-700 MB.

2. **Płyta CD-R** to optyczny nośnik danych, który może być jednokrotnie zapisywany w napędzie CD-ROM. Technologia ta polega na wykorzystaniu promienia lasera do trwałej zmiany właściwości optycznych niektórych punktów specjalnej substancji, znajdującej się pod przezroczystą akrylową powłoką płyty.
3. **Płyta CD-RW** to optyczny nośnik danych, który może być wielokrotnie zapisywany w specjalnym napędzie (nagrywarce). Technologia ta podobnie jak w przypadku dysku CD-R polega na wykorzystaniu promienia lasera, ale do odwracalnej zmiany właściwości optycznych płyty.
4. **Płyta DVD** – pomimo standardowych rozmiarów (120 mm średnicy) płyty DVD należą do nośników bardzo pojemnych. Technologia stosowana w przypadku tych płyt wykorzystuje światło lasera o krótszej fali niż w przypadku standardowych płyt kompaktowych. Dzięki temu możliwy jest gęstszy zapis na płycie. Nośnik danych jest również o połowę cieńszy, co pozwala złączyć jego dwie warstwy i utworzyć dysk dwustronny tej samej grubości co standardowa płyta CD. W przeciwieństwie do płyt CD-ROM dane na dysku DVD mogą być zapisywane dwuwarstwowo. Pozwala to uzyskać bardzo duże pojemności, nawet do 17 GB.
5. **Blu-ray** Disc (BD) – format zapisu optycznego będący następcą formatu DVD, od którego odróżnia się większą pojemnością płyt, co jest możliwe dzięki zastosowaniu niebieskiego lasera (w nagrywarkach DVD używany jest czerwony laser). Ten typ nośnika pozwala na zapisanie 25 GB danych na płytach jednowarstwowych, 50 GB na dwuwarstwowych.

Pojemności nośników danych

- Dyskietka 1,44 MB
- CD-ROM 700~800 MB (486~555 dyskietek)
- DVD-ROM 4,7 GB (3.342 dyskietki)
- Dysk twardy 500 GB (0,5 TB) (364.088.888 dyskietek)

Temat 6: Profilaktyka antywirusowa

Badware (złe, szkodliwe oprogramowanie) – jest ogólną nazwą oprogramowania mogącego wyrządzić szkody ich użytkownikom. Oprogramowanie takie składa się z kilku podgrup, a najliczniej reprezentowaną i najpopularniejszą stanowią wirusy komputerowe. Jest wiele rodzajów szkodliwych programów, które można podzielić na kilka kategorii:

- wirusy,
- konie trojańskie,
- robaki,
- króliki.

Czym jest wirus?

Wirus komputerowy to tak jak wirus grypy czy innej choroby atakującej człowieka. W komputerze tak jak i u człowieka, są wirusy powodujące poważniejsze choroby jak i te mało groźne. Każdy z nas choruje i głównie tylko od nas zależy jak często się to dzieje. Również od nas zależy jak często będzie „chorował" nasz komputer.

Wirusy komputerowe są to niewielkie programy, które nie są samodzielnymi, wykonywalnymi zbiorami. Każdy taki wirus musi mieć swojego nosiciela. Nosicielem może być w zasadzie każdy program użytkowy, program specjalny niewidoczny dla użytkownika lub jakikolwiek plik. Po dołączeniu się do programu wirus zmienia sposób jego funkcjonowania. W chwili uruchamiania zainfekowanego programu rozpoczyna się dwufazowy etap działania wirusa. Pierwszy to maksymalne rozmnożenie wirusa polegające na umieszczeniu wirusa w kolejnych miejscach systemu. Miejsca te są zależne od typu wirusa. Druga faza to destrukcyjne działanie wirusa. Najczęściej aktywowana ona jest w wyniku wystąpienia konkretnych warunków, głównie określonych przez twórców (np. wirus Czarnobyl, który uaktywniał się 26 dnia

każdego miesiąca na pamiątkę wybuchu w elektrowni w Czarnobylu). Działanie wirusów jest różnorodne – zależne od pomysłowości i fachowości jego twórców. Najbardziej szkodliwe są wirusy niszczące dyski twarde, unieruchamiające systemy, kasujące Bios komputera, itp.

Wirus komputerowy

Wirus komputerowy – to program, który – tak jak prawdziwy wirus – przyłącza się do innych programów i jest wraz z nimi przenoszony jest pomiędzy komputerami.

Miejsca w systemie komputerowym, które mogą być narażone na zainfekowanie wirusami:

- programy typu EXE, COM,
- biblioteki systemowe DLL,
- pliki systemowe np. COMMAND.COM,
- tablica partycji dysku twardego,
- boot sektor dysku lub dyskietki,
- dokumenty programu WORD, skoroszyty programu EXCEL (makropolecenia).

Typy wirusów

- dyskowe,
- plikowe.

Działanie wirusów

Wirus w fazie pierwszej (aktywacji) jest uruchamiany (uruchomienie „głowy” wirusa: w przypadku wirusów plikowych jest to uruchomienie zainfekowanego programu; w przypadku wirusów dyskowych polega na

uruchomieniu komputera z zarażonego nośnika). W fazie tej, głównym zadaniem wirusa jest rozmnażanie się i w miarę możliwości infekowanie jak największej ilości komputerów.

W drugiej fazie (destrukcji) wirus dokonuje zniszczeń w systemie (np. usuwa, modyfikuje pliki, zmienia nazwy, itp.). Jest to najniebezpieczniejsza część działalności wirusa. Faza ta jest opcjonalna, a niektóre wirusy na tym etapie kończą swoje działanie.

W ostatnim etapie (ujawnienia) użytkownik zostaje poinformowany o obecności obcego programu (np. odegranie melodyjki czy wyświetlenie komunikatu). Faza ta jest opcjonalna i nie musi wystąpić.

Fazy funkcjonowania wirusów

- faza rozmnażania się wirusa (tajna),
- faza destrukcji (jawna).

Rodzaje wirusów komputerowych

- **Łańcuch szczęścia** – jest to program zawarty w komunikacie wysyłanym pocztą elektroniczną, który po uruchomieniu wysyła kopie do wielu użytkowników.
- **Bomba logiczna** – wirus który uaktywni się gdy zostaną spełnione określone warunki logiczne (np. dojdzie do załamania sytemu gdy usuniemy określony plik),
- **Bomba czasowa** – wirus który uaktywnia się np. w ustalonych dniach (np. 13 dnia miesiąca czy w dniu urodzin autora wirusa),
- **Koń trojański** (trojan) – dowolny program, który zawiera kod realizujący funkcje inne niż spodziewa się tego użytkownik lub inne niż zawiera dokumentacja,

- **Robak** (worm) – program który wysyła swoje kopie przez połączenia sieciowe do innych komputerów. W odróżnieniu od wirusa, robak nie potrzebuje programu nosiciela, a jest samodzielnym programem wykonywalnym,
- **Królik** – czasem nazywany bakterią jest programem, który na skutek ciągłego powielania samego siebie (rozmnażania) wykorzystuje coraz większe zasoby komputera powodując jego destabilizację (zakłócanie – spowolnienie pracy).

Zagrożenia

Najpopularniejszymi szkodliwymi działaniami są:

- Instalowanie w systemie backdoor'a i udostępnianie kontroli nad systemem osobom trzecim w celu np. rozsyłania spamu,
- dokonywanie przez hackerów ataków DDoS, itp. (komputer-zombie),
- szpiegowanie i wykradanie poufnych danych użytkownika (spyware),
- utrudnianie pracy programom antywirusowym,
- zmiana strony startowej przeglądarki WWW i prezentowanie reklam,
- działania niszczące (kasowanie plików, uniemożliwianie korzystania z komputera).
- instalacja tzw. dialerów (zmiana dostawcy dostępu do Internetu).

Koń trojański

Koń trojański (ang. trojan horse) – to oprogramowanie, które podszywając się pod przydatne lub ciekawe dla użytkownika programy dodatkowo posiadają niepożądane, ukryte przed użytkownikiem funkcje. (Nazwa pochodzi od mitologicznego konia trojańskiego.) Np. umożliwia przechwycenie haseł czy znaków wprowadzanych z klawiatury. Program wykonuje najczęściej pożyteczne funkcje równocześnie realizując ukryte zadania (np. kasowanie

plików). Szkodliwość koni trojańskich polega na tym, że otwierają własny port, czyli rodzaj furtki do systemu i nasłuchują poleceń hackera. Trojan umożliwia hackerowi wykonywanie zdalnych poleceń na zainfekowanym komputerze (czytanie dokumentów, poczty e-mail, rozmów przeprowadzanych za pomocą komunikatorów internetowych (Gadu-Gadu), „podglądanie" ekranu monitora, obrazu z kamery internetowej czy dźwięku z podłączonego mikrofonu).

Konie trojańskie nie posiadają zdolności do samoistnego rozmnażania się (w przeciwieństwie do robaków (worm)), a ich aktywacja może nastąpić poprzez ich uruchomienie i spełnienie określonych warunków (wymuszenie na ofierze uruchomienia zainfekowanego trojanem pliku). Tak więc Koń trojański potrzebuje człowieka (hackera), który dostarczy go na komputer ofiary i po jego zainfekowaniu będzie sterował samym trojanem.

Jak następuje infekcja?

Wirusy rozpowszechniają się najczęściej za pośrednictwem poczty elektronicznej (list z zarażonym załącznikiem). Uruchomienie załącznika powoduje zawirusowanie komputera i najczęściej rozesłanie wirusa bez wiedzy użytkownika do wszystkich osób, których adresy e-mailowe znajdują się w książce adresowej programu pocztowego lub innej bazie zawierającej adresy (np. w pliku Worda).

Nie istnieje coś takiego jak pełna ochrona antywirusowa. Komputer można zainfekować nie tylko poprzez pocztę elektroniczną, ale także korzystając z różnego rodzaju nośników danych niewiadomego pochodzenia możemy narazić nasz komputer na zarażenie groźnym wirusem. Należy także liczyć się z faktem, iż ściągane przez nas pliki z sieci, bądź też kopiowane zbiory z lokalnej sieci mogą być zainfekowane. Co więcej, jeśli komputer jest podłączony do sieci, wirusy (robaki) mogą dostać się do naszego systemu bez żadnej „pomocy" z naszej strony!

Najskuteczniejszym sposobem na ustrzeżenie się przed wirusami jest sprawdzanie plików (dokumenty, programy) programem antywirusowym z jak najnowszą bazą danych sygnatur.

Nie ma zasad, gwarantujących bezwirusową pracę. Istnieją jednak reguły, pozwalające zminimalizować ryzyko zarażenia, a w razie infekcji zmniejszające skutki niszczycielskich działań wirusa.

Podstawową metodą obrony przed oprogramowaniem tego typu powinna być profilaktyka.

Profilaktyka (zapobieganie zarażeniom)

Profilaktyka antywirusowa polega na:

- ostrożnym postępowaniu z załącznikami z podejrzanych wiadomości e-mail i innym oprogramowaniem nieznanego pochodzenia,
    - nie należy otwierać załączników otrzymanych w listach od nieznajomych
    - należy usuwać bezzwłocznie e-maile z załącznikami w sytuacji, gdy otrzymamy je od nieznanych nadawców
- używanie legalnego oprogramowania,
- używanie oprogramowania antywirusowego (programów antywirusowych),
- częsta aktualizacja baz wirusów (sygnatur wirusów) programu antywirusowego,
- używanie programów antyspyware,
- używanie zapory sieciowej – firewalla (uniemożliwiającego dostęp do komputera od strony Internetu),
- systematycznym aktualizowaniu systemu operacyjnego i przeglądarek internetowych,

- regularne tworzenie kopii bezpieczeństwa najważniejszych danych (najlepiej na wyjmowanym nośniku danych, np. pendrive lub na płytach CD lub DVD),
- wkładając cudze nośniki danych do swojego komputera, należy je sprawdzić programem antywirusowym z aktualną bazą wirusów.

Wykrywanie wirusów

Wykrywanie wirusów - Aby wykryć wirusy stosuje się następujące metody:

1. Poprzez sumę kontrolną
   - Przed zarażeniem sprawdza się wielkość plików.
   - Zarażenie zmienia wielkość pliku zarażonego (kod wirusa posiada przecież określoną wielkość).

     Nieskuteczność tej metody polega na tym, że:

     a. niektóre wirusy potrafią ukrywać swoją wielkość,

     b. dokumenty zmieniają swoją wielkość podczas ich edycji.
2. Poprzez kod wirusa
   - Wyodrębnienie z nosiciela kodu wirusa.
   - Sprawdzać czy inne pliki nie posiadają na końcu lub na początku takiego kodu.
   - Po usunięciu wirusa mówimy że plik zarażony został odwirusowany lub wyleczony.

Program antywirusowy

Programy antywirusowe – to specjalne programy, które sprawdzają programy w komputerze i dane na dysku oraz na dyskietkach, pendrive'ach, płytach CD i jeśli znajdą wirusy, starają się je unieszkodliwić oraz wyleczyć zarażone pliki.

Aby zwalczyć nowo powstałe wirusy, programy antywirusowe muszą być często uaktualniane. (Czyli muszą posiadać jak najświeższe tzw. sygnatury baz

wirusów (tzw. próbki wirusów), gdyż każdego dnia na świecie pojawiają się setki nowych wirusów, a ich rozprzestrzenianie poprzez sieć Internet odbywa się w sposób błyskawiczny.)

Haker

Haker (ang. hacker) – czyli włamywacz – osoba, która szuka i ewentualnie wykorzystuje dziury w zabezpieczeniach oprogramowania komputerowego. Może też dzięki nim uzyskiwać dostęp do zabezpieczonych komputerów. Najwyższym poziomem umiejętności cechują się ci spośród hakerów, którzy opracowują nowe, nieznane dotąd metody ataków.

Umiejętności: Szczególnym zainteresowaniem hakerów cieszą się następujące zagadnienia:

- luki (dziury) w:
  - systemach operacyjnych (Windows, Linux, Unix),
  - programach,
  - sieciach komputerowych (systemy zabezpieczeń),
  - urządzeniach (głównie podłączonych do sieci, ale również m.in. w telefonii),
  - systemach autoryzacji (kontrola dostępu do zasobów),
- (zdalne) przejmowanie kontroli nad danym systemem (zdobywanie uprawnień nadzorcy systemu),
- techniki (elektronicznego) kamuflażu oraz zacierania śladów,
- zaawansowana znajomość technik agresji teleinformatycznej (np. sniffing, podszywanie się, tworzenie koni trojańskich.),
- budowa i funkcjonowanie systemów operacyjnych.

Cele: Hakerzy-włamywacze działają z różnych pobudek: dla niektórych jest to chęć zysku możliwego do uzyskania przy pomocy wykradzionych danych, dla

innych uzyskanie rozgłosu i wywołanie zamieszania. Część z nich twierdzi, że włamując przyczynia się do zwiększenia dbałości administratorów o zabezpieczenia.

Aspekt prawny

Przestępstwa komputerowe a prawo karne:

„Kto bez uprawnienia uzyskuje informację dla niego nieprzeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". (Artykuł 267 § 1 kodeksu karnego.)

Przestępstwa przeciwko ochronie informacji:

- Hacking – do 2 lat więzienia
- Podsłuch i inwigilacja – do 2 lat więzienia
- Niszczenie danych komputerowych – od 2 do 3 lat więzienia
- Sabotaż komputerowy – od 6 miesięcy do 8 lat więzienia

Przestępstwa przeciwko mieniu:

- Nielegalne używanie programu komputerowego – od 3 miesięcy do 5 lat więzienia
- Paserstwo (kupno nielegalnego) programu komputerowego – od 3 miesięcy do 5 lat więzienia
- Oszustwo komputerowe – od 3 miesięcy do 5 lat więzienia

Inne rodzaje przestępstw:

- Szpiegostwo komputerowe – do 25 lat więzienia

Temat 7: Poznajemy system operacyjny MS Windows

System operacyjny

System operacyjny (ang. skrót OS – Operating System) – oprogramowanie zarządzające sprzętem komputerowym, tworzące środowisko do uruchamiania i kontroli zadań użytkownika (programów użytkowych).

Systemy z rodziny Windows posiadają środowisko graficzne ułatwiające komunikację pomiędzy komputerem z użytkownikiem.

Panel sterowania

Panel sterowania – aplikacja (program) systemowa w systemach operacyjnych Microsoft Windows, gromadząca w jednym miejscu narzędzia do ustawiania i zmiany parametrów systemu operacyjnego.
Panel sterowania umożliwia zarządzanie różnymi kategoriami sprzętu, usług i programów oraz kontami użytkowników. Zmiany tu wprowadzone zwykle dotyczą całego systemu i są istotne dla jego sprawnego działania.

Eksplorator Windows

Eksplorator Windows – aplikacja (program) do przeglądania systemu plików w Microsoft Windows. Eksplorator jest także domyślną powłoką tych systemów operacyjnych. Powłoka pokazuje ikony na pulpicie, a także pasek zadań.
Możemy go uruchomić poprzez jednoczesne wciśnięcie klawiszy Logo Windows i E na klawiaturze.

Okno Eksploratora podzielone jest na dwa pionowe segmenty. Część lewa przedstawia hierarchiczne drzewo zasobów dyskowych komputera (foldery, dyski lokalne), natomiast część prawa wyświetla zawartość folderu zaznaczonego po lewej stronie.

Główne zadania systemu operacyjnego

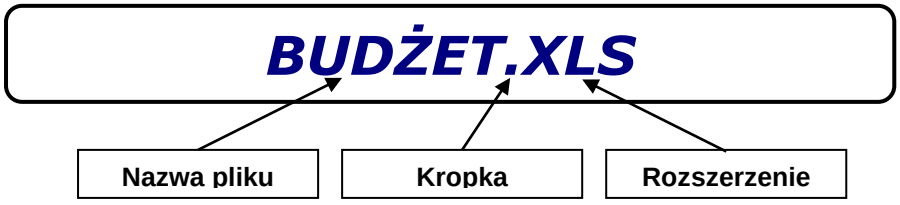
- zarządzanie uruchomionymi programami
- zarządzanie pamięcią operacyjną
- zarządzanie plikami
- zarządzanie urządzeniami wejścia/wyjścia
- zarządzenie nośnikami danych

Ważniejsze systemy operacyjne

- BeOS
- OS/2
- NetWare
- MS-DOS
- Linux
- Microsoft Windows:
  - Windows 3.1
  - Windows 3.11
  - Windows 95
  - Windows 98
  - Windows Millenium,
  - Windows NT 4.0
  - Windows 2000
  - Windows XP
  - Windows 2003

- Windows Vista
- Windows 7
- Windows 8.1
- Windows 10

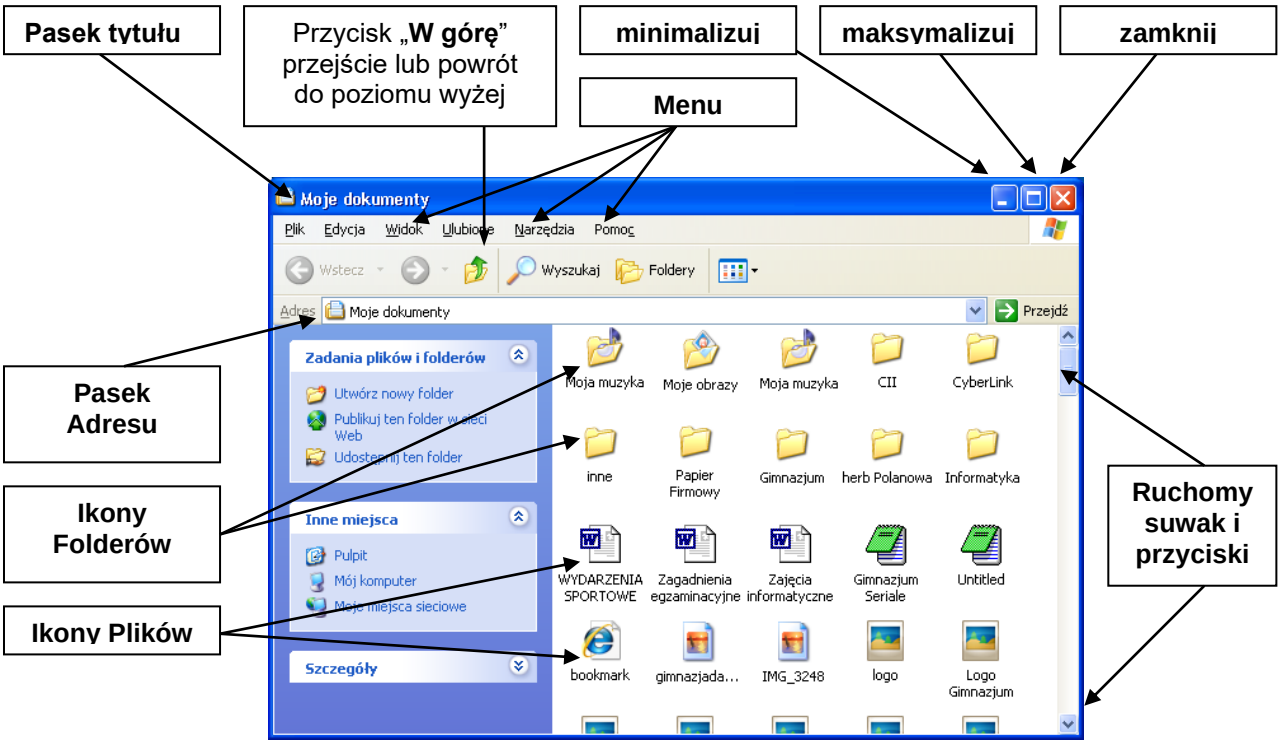
Budowa nazwy pliku



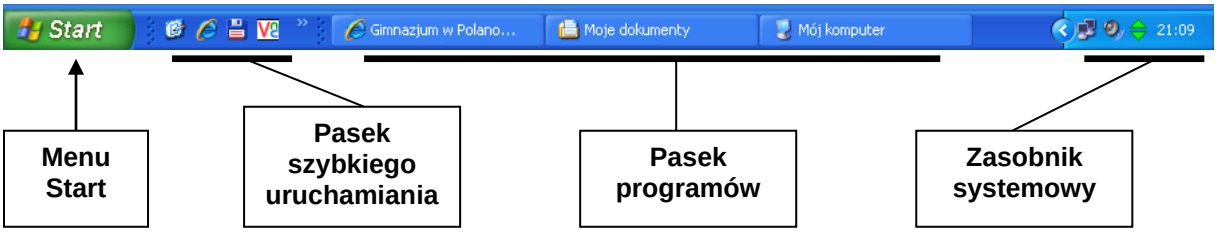
Rodzaje plików

Rodzaj pliku	Rozszerzenie
tekstowe	TXT, DOC
dźwiękowe	WAV, MP3
filmowe	AVI, MPG
graficzne	JPG, GIF, BMP
wykonywalne	EXE, COM, BAT

Budowa okna



Pasek zadań



Temat 8: Sieci komputerowe.

Rodzaje sieci

Sieć – (ang. network) to zespół komputerów lub innych urządzeń połączonych ze sobą w taki sposób, że możliwa jest wymiana informacji między nimi.

Sieci kablowe – to sieci, w których do połączenia komputerów i transmisji danych został wykorzystany kabel. Może to być tzw. skrętka, kabel koncentryczny lub światłowód.

Zalety:

- niskie koszty instalacji,
- odporność na uszkodzenia mechaniczne i zakłócenia.

Wady:

- trudność w zlokalizowaniu uszkodzenia kabla lub unieruchomienie całego odcinka sieci w razie awarii

Sieci bezprzewodowe – charakteryzują się brakiem połączeń kablowych. Transmisja odbywa się za pomocą fal radiowych lub podczerwieni.

Zalety:

- brak kabli,
- możliwość przemieszczania komputerów i całej sieci.

Wady:

- ograniczenia zasięg sieci,
- wrażliwość na zakłócenia,
- łatwość przechwycenia przesyłanych danych przez osoby niepożądane.

Topologia sieci

Topologia sieci – to sposób fizycznego połączenia komputerów w sieć na określonym obszarze.

Podstawowe topologie sieci

- magistrala (szyna),
- gwiazda,
- pierścień.

Sposoby łączenia komputerów w sieć

Topologia magistrali (szyny) – polega na podłączeniu kolejnych komputerów do jednego kabla (BNC) za pomocą tzw. trójników (T-Conector). Na końcu kabla umieszcza się tzw. terminatory blokujące odbicia sygnału.

Zalety:

- prosty sposób instalacji,
- odporność na zakłócenia,
- możliwość łączenia komputerów na znacznych odległościach (max 185 m)

Wady:

- duża awaryjność (uszkodzenie kabla rozłącza całą sieć),
- niska prędkość transmisji danych (max 10 Kb/s)

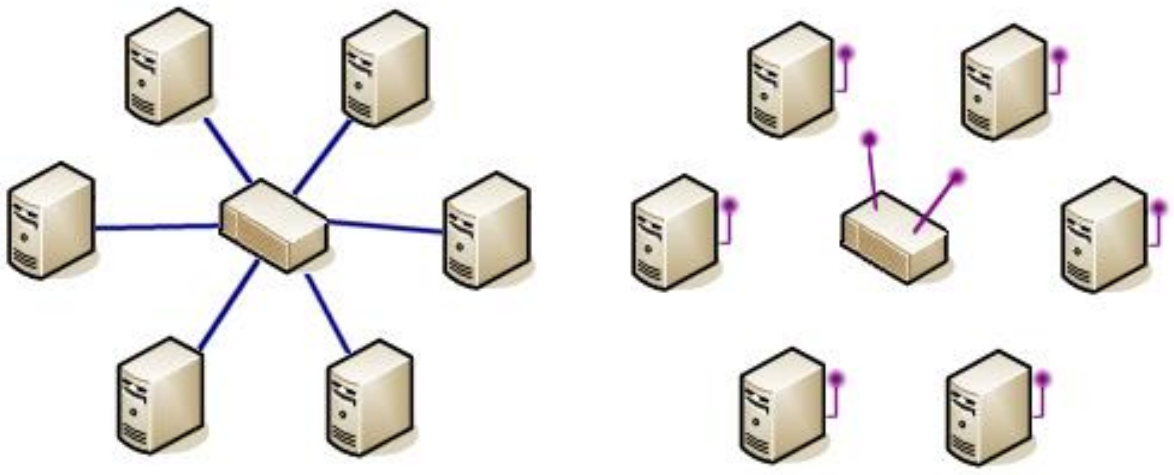
Topologia gwiazdy – to podłączenie poszczególnych komputerów do jednego urządzenia, którym może być koncentrator (ang. hub) lub przełącznik (ang. switch).

Zalety:

- możliwość dołączania w dowolnym czasie innych komputerów,
- szybka lokalizacja awarii,
- wysoka prędkość transmisji danych (od 10 ~ 1000 Mb/s)

Wady:

- konieczność wykorzystana dużej ilości okablowania (8. żyłowy kabel UTP tzw. „skrętka”),
- ograniczenia dot. odległości pomiędzy komputerami (max 90 m),
- w przypadku sieci radiowych – podatność na przeszkody terenowe, zakłócenia sygnału i możliwość łatwego podsłuchu.

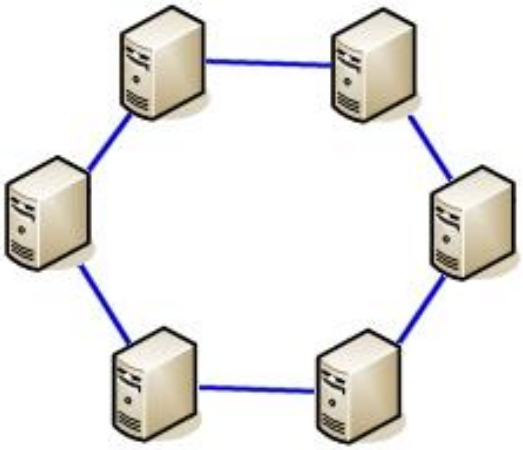


Topologia pierścienia (ang. **token ring)** – okablowanie nie ma żadnych zakończeń (tworzy krąg). Metoda transmisji danych w pętli polega na przekazywaniem żetonu dostępu. Przejęcie żetonu zezwala urządzeniu na transmisję danych. Sieć posiada tylko jeden żeton.

Wady:

- awaria pojedynczego przewodu lub komputera powoduje przerwanie pracy całej sieci,
- trudna lokalizacja uszkodzenia,

- dołączenie nowych stacji jest utrudnione.



Budowa sieci

Do utworzenia sieci niezbędne jest:

- zamontowanie karty sieciowej,
- zamontowanie okablowania,
- zainstalowanie sterownika karty sieciowej,
- zainstalowanie protokołu sieciowego (np. TCP/IP),
- zainstalowanie oprogramowania klienta sieci oraz usługi.

Protokół sieciowy – (ang. network protocol) to zbiór reguł obowiązujących w sieci, np. sposób adresowania czy kontrola poprawności transmisji danych.

TCP/IP – umożliwia komunikowanie się komputerów w Internecie. Każdy komputer pracujący w sieci ma przypisany indywidualny (i niepowtarzalny!) adres IP w postaci 4 liczb z zakresu od 0 do 254 oddzielonych kropkami, np. 83.19.189.18.

Podział sieci

Ze względu na zasięg:

- Sieci lokalne **LAN** (ang. Local Area Network) – to komputery połączone w obrębie jednego budynku, np. biura, szkoły, przedsiębiorstwa.
- Sieci miejskie **MAN** (ang. Metropolitan Area Network) – to komputery obejmujące swym zasięgiem miasto lub osiedle.
- Sieć rozległa **WAN** (Wide Area Network) – ogólnoświatowa sieć rozległa np. Internet lub sieci korporacyjne.

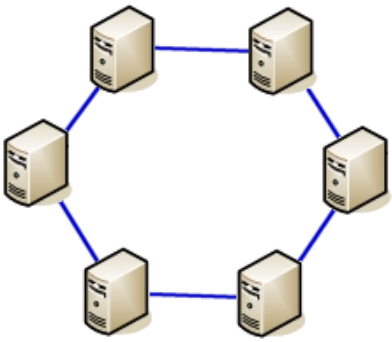
Ze względu na zarządzanie zasobami:

- **każdy z każdym** (peer to peer / P2P) – to połączenie zapewniające pracę wszystkich komputerów na równych zasadach oraz możliwość korzystania z zasobów innych komputerów i drukarek. Taka sieć nie wymaga administrowania.
- **klient-serwer** – wyznaczony jest jeden komputer do pełnienia nadrzędnej funkcji – serwera. Na nim instaluje się sieciowy system operacyjny i przechowuje dane oraz programy udostępniane stacjom roboczym (klientom). Osoba nadzorująca pracę serwera i sieci to administrator. Administrator przyznaje poszczególnym użytkownikom określone prawa do korzystania z danych zasobów.

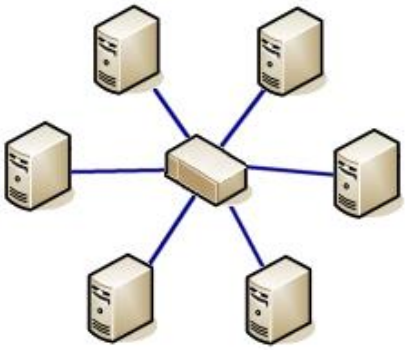
Ze względu na medium transmisyjne:

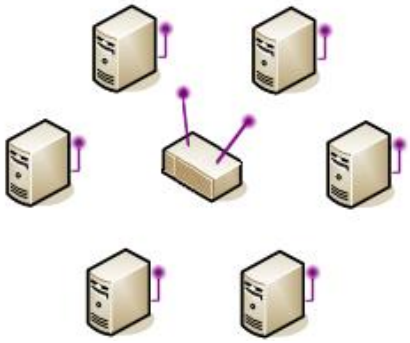
- Sieć radiowa **W-LAN** (Wireless - Local Area Network) – lokalna sieć oparta na technologii Wi-Fi (połączenia radiowe).

✂----------

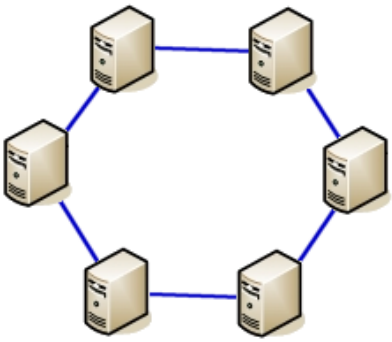


✂----------

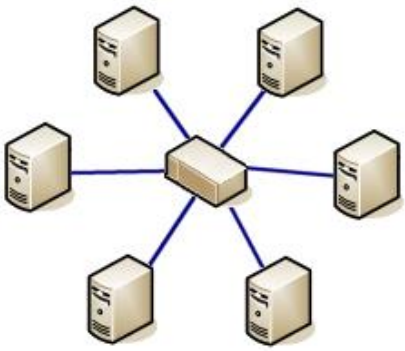


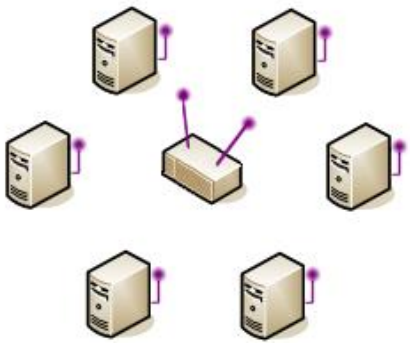


✂----------



✂----------





✂----------