## Informácia, informatika

### Údaj, informácia

Informácia je údaj či správa, ktorý nás vedie z nevedomosti do vedomosti. Niečo, čo nám poskytuje nejakú vedomosť či údaj. Informácie sú podmnožina údajov. Rozdiel medzi údajom a informáciou je, že údaj nás nemusí uviesť do vedomosti, správu údaju môžeme už poznať a teda nepovie nám nič nové.

### Informatika

Informatika sa zaoberá informáciami, ich získavaním, ukladaním, spracovaním a šírením. Zaoberá sa tiež algoritmami a ich realizáciou na počítači. Algoritmus (program) je presný postup na riešenie nejakej úlohy.

### Typy informácií

* Obrázok – napr. dopravná značka alebo fotka
* Text – napr. Wikipédia
* Zvuk – napr. výklad
* Video
* Čísla
* Tabuľka
* Gestá

Nástrojom na spracovanie informácií je počítač.

### Jednotky informácii

**Základnou jednotkou informácie je jeden bit. Bit môže byť 1 alebo 0.** Na mieste kde je jeden bit a je tam dohodnuté napätie je to 1. Ak tam nie je napätie jeden bit sa rovná 0. 1 Byte je 8 bitov. 1B=8b.

* 1 kJ = 1000 J = 1 \* 103 J
* 1 MJ = 100000 J = 1 \* 106 J
* 1 GJ = 100000000 J = 1 \* 109 J
* 1 KiB = 1024 B = 210 B
* 1 MiB = 220 B
* 1 GiB = 230 B

## Číselné sústavy, prevody

Dvojková sústava je číselná sústava, v ktorej sa číslo zapisuje pomocou 0 a 1. V desiatkovej sústave sa číslo zapisuje pomocou 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Prevod čísla z desiatkovej do dvojkovej sústavy:

1. spôsob pomocou delenia 2 2. spôsob

11/2=5 zv. 1 8 4 2 1

5/2=2 zv. 1 1 0 1 1

2/2=1 zv. 0 11-8=3

1/2=0 zv. 1 3-2=1

1110=10112 1-1=0

### Priamy kód

Prvý (najvýznamejší) bit čísla, ktoré zapisujeme teda dostane hodnotu podľa toho, či je číslo kladné alebo záporné. 0 na začiatku čísla znamená, že bude kladné a 1 znamená, že bude záporné. Bez znamienka môžeme vyjadriť hodnoty od 0 po 2n−1, priamym zápisom môžeme vyjadriť interval od −2n−1 po 2n−1.

### Inverzný kód

Inverzný kód binárneho čísla sa vytvorí tak, že sa každá jedna číslica v binárnom čísle neguje (to znamená že z jednotiek budú nuly a z núl sa stanú jednotky), pričom musí byť vopred známy počet bitov vyhradený pre túto reprezentáciu čísel.

### Doplnkový kód

Doplnkový kód binárneho čísla sa vytvorí tak, že sa k inverznému kódu čísla pripočíta jednotka. A zase: pri vopred dohodnutom počte bitov.

## Digitalizácia

### Digitalizácia textu

* Každé písmeno/znak musí mať nejaký kód
* Kódovacia tabuľka
* ASCII - Iba znaky v americkej abecede
* Každý znak zaberal sedem bitov
* Potom vznikli národné tabuľky
* Národná tabuľka = ASCII + ďalších 128 národných znakov
* Jeden znak v národnej tabuľke = 8 bit
* UNICODE – všetky znaky sveta
* Jeden znak má 16 bitov
* Má 65536 znakov
* UTF 8 - Kód na šetrenie pamäte, pre územie strednej Európy
* Znaky v ASCII – 8 bit
* Národné – 16 bit

### Digitalizácia obrázkov

* 2 spôsoby: 1) bitová mapa (rastrový obrázok) – obrázok je rozdelený pomocou mriežky (raster) na pixely (obrazové body), každý pixel má jednu farbu a tá sa zakóduje na číslo a do počítača uložíme jednotlivé kódy zľava doprava po riadkoch. Rozlíšenie – počet pixelov (šírka x výška), farebná hĺbka – počet bitov, ktoré potrebuje na uloženie jedného pixelu

1b – sme schopní uložiť 2 farby (0 – čierna, 1 – biela)

2b – 4 farby (00, 01, 10, 11)

3b – (000, 001, 010, 011, 100, 101, 110, 111)

Počet farieb – 2 na počet bitov

R G B

255 255 255

11111111 11111111 11111111

FF FF FF biela

00 00 00 čierna

FF 00 00 červená

00 FF 00 zelená

00 00 FF modrá

FF FF 00 magenta (purpurová)

00 FF FF cyan (azúrová)

FF FF 00 yellow (žltá)

* CMY – tlačiareň (CMYK), K – blacK
* sivá rovnaký pomer R, G, B
* Komprimovaný obrázok – menej bitov: .png, .jpg (úsporne uložený)

2) vektorový obrázok – skladá sa z kriviek, objektov. Ukladá sa len (veľkosť, poloha, farba), nezobrazujú reálny svet, pri zmene veľkosti nemenia kvalitu

**Príklad:**

1024 x 768

Farebná hĺbka – 24 bitov

2,25 MiB

### Digitalizácia zvuku a videa

### Zvuk

1. Vzorkovanie – meria zvukové vlny vytvára vzorky (b) – (.wav)
   1. Frekvencia vzorkovania (Hz) je počet vzoriek za sekundu = 8000 – 48 000 Hz
   2. Veľkosť nahrávky (b) = vzorka (b) \* frekvencia vzorkovanie (s-1) \* dĺžka nahrávky (s) \* počet kanálov
   3. Stereo – dva kanály, mono – jeden kanál
   4. Kompresia – zmenší sa objem bitov – stratová (.mp3)
   5. Kód = viac vzoriek samplovanie
2. Umelý zvuk – vznikol elektronicky - MIDI
   1. Monofónny – jeden nástroj
   2. Polyfónny – viac nástrojov, 100010
   3. Obrázok, na ktorom je rad, vývoj, diagram, text

      Automaticky generovaný popisNoty kód

### Video

* Obrázky - zvuk – kontajner (.avi)
* Veľkosť videonahrávky = rozlíšenie obr. \* farebná hĺbka \* čas (s) \* frekvencia (s-1)
* Komprimácia – zníženie FPS a zhoršenie rozlíšenia (.mp4)

### Kompresia

Zmenšenie veľkosti súborov

Kompresný pomer – pomer veľkosti skomprimovaného a neskomprimovaného súboru

Kompresia:

* **stratová** – úspornejšie uloženie pôvodných údajov, pričom sa časť informácie zanedbáva (nízke tóny pri MP3, niektoré farebné odtiene spriemerované pri formáte JPG).
* **bezstratová** – iný spôsob uloženia pôvodných údajov, pričom pôvodné údaje sa dajú zrekonštruovať bez straty kvality.

## 4. Hardvér

Obrázok, na ktorom je text, snímka obrazovky, diagram, písmo

Automaticky generovaný popis

### Podľa tejto schémy sa počítač skladá z piatich hlavných modulov:

**Operačná pamäť** : slúži na uloženie spracovávaného programu, spracovávaných údajov a výsledkov výpočtu.

**ALU - aritmeticko-logická jednotka**: jednotka vykonávajúca všetky aritmetické výpočty a logické operácie. Obsahuje sčítačky, násobičky (na aritmetické výpočty) a komparátory (na porovnávanie).

**Riadiaca jednotka**: riadiaca jednotka, ktorá riadi činnosť všetkých častí počítača. Toto riadenie sa vykonáva pomocou **riadiacich signálov, ktoré** sa posielajú jednotlivým modulom. V reakcii na riadiace signály sa stavy jednotlivých modulov zasa posielajú späť do riadiacej jednotky prostredníctvom **stavových správ**

**Vstupné zariadenie**: zariadenie určené na vstup programu a údajov.

**Výstupné zariadenie**: zariadenie určené na výstup výsledkov spracovaných programom.

Vo von Neumannovej schéme možno označiť ďalšie dva moduly, ktoré vznikli zjednotením predchádzajúcich modulov:

**Procesor**: kontrolér + ALU

**CPU - centrálna procesorová jednotka**: CPU + RAM

1. Program, ktorý bude vykonávať výpočet, sa umiestni do operačnej pamäte pomocou vstupných zariadení prostredníctvom ALU.
2. Rovnakým spôsobom sa do operačnej pamäte umiestnia údaje, ktoré má program spracovať
3. Prebieha vlastný výpočet, ktorého jednotlivé kroky vykonáva ALU. Túto jednotku spolu s ostatnými modulmi počas výpočtu riadi riadiaca jednotka počítača. Medzivýsledky výpočtu sa ukladajú do operačnej pamäte.
4. Po dokončení výpočtu sa výsledky odošlú prostredníctvom ALU do výstupného zariadenia.

## 5. Konfigurácia počítača PC

### Osobný počítač

Osobný počítač je počítač určený pre osobné použitie, pre použitie jednotlivcom. Tento názov vznikol v čase, keď boli počítače väčšinou veľké (sálové, strediskové a pod.) a ich čas sa zdieľal medzi viacerých používateľov. Tento termín sa začal používať na konci sedemdesiatych a začiatkom osemdesiatych rokov minulého storočia, kedy sa prvé počítače dostali do domácností. Prechod zo sálového do domáceho prostredia spôsobil aj zmenu v chápaní počítača z vedeckého ponímania (počítač na vedecké výpočty) na zábavné zariadenie. Dnešné osobné počítače sa v prvom rade používajú ako domáce zábavné elektrospotrebiče s prístupom na internet, schopnosťou prehrávať a modifikovať multimediálny obsah.

### Pracovná plocha osobného počítača

Pracovná plocha predstavuje hlavnú časť obrazovky, ktorá sa zobrazí po spustení počítača a prihlásení do systému Windows. Plní funkciu pracovnej plochy podobne ako skutočný pracovný stôl. Na pracovnej ploche sa zobrazí každý otvorený program alebo priečinok. Môžete na ňu umiestniť jednotlivé položky, napríklad súbory a priečinky a usporiadať ich podľa svojho želania.

### Funkcia a parametre jednotlivých komponentov počítačov PC

Procesor – počet jadier, vlákien, frekvencia, veľkosť vyrovnávacej pamäte – cache

Monitor – rozlíšenie, obnovovacia frekvencia, typ pripojenia (napr. HDMI)

Pamäť RAM – veľkosť operačnej pamäte

Pevný disk – HDD alebo SSD

## 6. Periférne zariadenia počítačov PC

### Definícia

Periférne zariadenie alebo tiež periféria je komponent, ktorý priamo nie je celistvou súčasťou výpočtového zariadenia. Nezúčastňuje sa teda na spracovaní informácií. Má však samozrejme možnosť byť k systémovej jednotke dodatočne pripojený.

### Rozdelenie

Periférie podľa ich funkcie rozdeľujeme na tri skupiny:

1. **Vstupné zariadenia (Input)**

Umožňujú vstup informácií do základnej jednotky počítača, ktoré sú potrebné na spracovanie. **Štandardnými vstupnými zariadeniami** sú klávesnica a myš. Používaním klávesnice vkladáme text, príkazy, a tak ovládame počítač. Klávesnica môže byť káblová alebo bezdrôtová. Myš je rýchlym ovládacím prvkom počítaču. Pohyb našej ruky je prenášaný pomocou špeciálnych senzorov a kliknutím tlačidiel myši spúšťame alebo ukončujeme rôzne funkcie počítača. Okrem klávesnice a myši sú **ostatné vstupné zariadenia**: hlasový vstup - mikrofón, grafický tablet, skener, gamepad (napr. joystick) a mnohé iné.

1. **Výstupné zariadenia (Output)**

Umožňujú výstup výsledkov spracovania informácií základnej jednotky počítača. **Štandardné výstupné:** monitor. Medzi **ostatné výstupné zariadenia** patria: tlačiareň, reproduktor, dataproduktor, plotter (veľkorozmerná tlač), 3D tlačiareň a iné. Displej (zobrazovacia jednotka) nám zobrazuje na obrazovke prijaté výsledky. V dnešnej dobe majú nejakú formu displeja všetky osobné počítače. Uhlopriečka v palcoch. Reproduktor nám prehráva informácie v zvukovej podobe. Podobne ako displej je reproduktor veľmi rozšírený. A napokon tlačiareň je veľmi rozšírená v domácom, ale hlavne v kancelárskom prostredí. Tlačiarní je viacero druhov (ihličková – napr. bloček v obchode, atramentové – CMYK, laserová – farba sa „priškvarí“), ale princíp zostáva rovnaký - informácie sú rôznymi spôsobmi prenesené na tlačové médium.

1. **Vstupno-výstupné zariadenia**

Sú to pokročilejšie zariadenia, ktoré umožňujú vykonať vstupnú a aj výstupnú funkciu. Najznámejšími zástupcami tejto skupiny napr. dotykový monitor, modem (modulátor, demodulátor).

1. **Multifunkčné zariadenia**

Je to spojenie výstupného a vstupného zariadenia do jedného. Nejedná sa však o vstupno-výstupné zariadenie. Napr. skener + tlačiareň.

## 7. Softvér počítačov PC

### Softvér

označuje programové vybavenie počítača – čiže všetky aplikácie, ktoré sa dajú na počítači spustiť. Softvér má na rozdiel od hardvéru nemateriálnu podobu. Medzi softvér zaraďujeme operačné systémy a ovládače zariadení, všetky druhy aplikačných programov, napríklad textové editory/procesory a iné kancelárske aplikácie, grafické aplikácie, aplikácie na prehrávanie multimédií, hry a všetky ostatné programy.

### Vzťah medzi hardvérom a softvérom

Hardvér je fyzická časť počítača, ako napríklad procesor, pamäť, pevný disk, grafická karta, klávesnica či monitor. Naopak softvér je programovateľná časť počítača, ktorá riadi chod hardvéru a umožňuje ho využiť na plnenie konkrétnych úloh. **Vzťah medzi hardvérom a softvérom je taký, že bez hardvéru nie je možné realizovať žiadne softvérové operácie a bez softvéru by hardvér bol iba nevyužitou súčasťou počítača.** Softvér riadi činnosť hardvéru a umožňuje používateľovi vykonávať rôzne úlohy a operácie pomocou počítača. Bez správnej komunikácie medzi hardvérom a softvérom by efektívne fungovanie počítačového systému nebolo možné. Preto je dôležité, aby softvér bol optimalizovaný pre konkrétny hardvér a naopak, aby hardvér bol schopný podporovať a pracovať s daným softvérom.

### Druhy softvéru

1. Systémový softvér – zabezpečuje spúšťanie ďalších aplikácií. Sú to napr. operačné systémy
2. Aplikačný softvér (aplikácie) – skupina programov určená na riešenie problémov. Zahŕňame sem napr. textové a grafické editory, prehliadače webových stránok atď.

### Typy licencií

Shareware – umožňuje bezplatné a legálne využívanie komerčne šíriteľného softvéru s určitými obmedzeniami. Patria sem:

* demoverzie – programy sa odomknú až po zadaní registračného kódu získaného zaplatením požadovanej čiastky.
* trialware – časovo obmedzené programy, umožňujú využívať softvér len niekoľko dní, alebo niekoľko spustení
* adware – zobrazovanie reklamy

Freeware – je softvér, ktorý môžeme používať a rozširovať zdarma, pričom sa dožaduje dodržiavanie autorských práv

* + betaverzie / testovacie verzie/ - sú špeciálny prípad freewaru, autor vytvorí niekoľko testovacích verzií nového programu, ktoré môže záujemca zdarma používať. Autor si vďaka nim overuje, ako program funguje, odstraňuje chyby. 3.

Public domain / verejné voľné dielo/ - predstavuje dielo, ktorého majetkové a autorské práva nie sú chránené. Možno s ním ľubovoľne narábať, rozmnožovať ho , meniť jeho zdrojové kódy. Open-source – je skupina voľne šíriteľného a modifikovateľného softvéru, ktorý môžeme ľubovoľne krát inštalovať, kopírovať a distribuovať, meniť jeho zdrojové kódy a modifikované výsledky zverejňovať.

Komerčný sofware - je vyvíjaný a predávaný komerčne, žijú z neho jeho tvorcovia, distribútori.

### Softvérová licencia

Softvérová licencia poskytuje právo legálne inštalovať, používať, pristupovať, zobrazovať, spúšťať, alebo inak pracovať so špecifickým softvérovým programom. Niekedy by ste mohli potrebovať licenciu pre každý počítač alebo zariadenie, na ktorom je daný softvér nainštalovaný. Licencia pokrýva rôzne práva, napríklad právo na downgrade alebo špecifikácie, či je licencia trvalá alebo dočasná.

## 8. Operačný systém

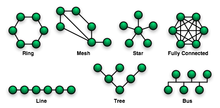
Operačný systém (OS) je súhrnné označenie pre programy, ktoré zabezpečujú komunikáciu medzi užívateľom a počítačom, riadia a dozerajú na spúšťanie a vykonávanie používateľských programov, prideľovanie prostriedkov jednotlivým programom a riadi tiež spôsob ukladania údajov.

1. jednoužívateľské / viacužívateľské

2. jednoúlohové / viacúlohové

1. Multitasking - súbežné vykonávanie viacerých úloh.
2. Rozšíriteľnosť -
3. Kompatibilita -
4. Záloha a obnova -
5. Lokalizácia - prispôsobovanie počítačových programov pre rôzne prostredie, najčastejšie iba preloženie do iného jazyka.
6. Plánovanie procesov - Úlohou plánovača (scheduler) je vybrať z radu pripravených procesov ten, ktorý sa bude vykonávať.
7. Multiprocessing – súbežné spracovanie viacerých úloh alebo podúloh. Systému s viacerými procesormi schopnému spracovávať viacero úloh súčasne hovoríme viacprocesorový systém.

## 9. Počítačová sieť

* Minimálne dva počítače PC a prepojíme ich medzi sebou, môže to byť nejaký kábel alebo to môže ísť vzduchom (Bluetooth) – môže tam v siete byť pripojené aj sieťové zariadenie, ktoré tam môže byť, ale nemusí
* Výhody počítačovej siete:
  + Zdieľanie
    - súborov, programov
    - hardvéru (disk, tlačiareň)
    - internetového pripojenia
* jednotná inštalácia, jednotný prístup
* komunikácia
* Nevýhody počítačovej siete:
  + Pri útoku na jeden počítač sú ohrozené všetky počítače v sieti aj ostatné PC
* **Sieťové zariadenia -** všetky zariadenia pripojené do počítačovej siete, ktoré prijímajú a vysielajú dáta (datagramy) z (do) počítačovej siete. (segment = časť)
  + Repeater – opakovač – obnovuje signál, ktorý na fyzicky dlhšom úseku siete degraduje, stráca pôvodné charakteristiky (silu a tvar)
  + Hub – rozbočovač – spája niekoľko segmentov siete do segmentu jedného (prevádzka v jednej časti siete sa prenesie aj do častí ďalších sietí)
  + Bridge – most – spája dva fyzicky oddelené segmenty siete
  + Switch – prepínač – spája dve a viac zariadení v rámci jedného alebo viacerých segmentov siete, oddeľuje sieťovú prevádzku (nezaťažuje ostatné časti siete)
  + Router – smerovač – presmerováva komunikáciu do iného segmentu rovnakého typu siete
  + Gateway – brána – sprostredkováva komunikáciu dvoch odlišných typov siete
* **Topológia siete** – akým spôsobom môžeme rozmiestniť počítače do siete, najpoužívanejší je bus, tree sa využíva často vo firemnom prostredí
* Delenie podľa rozľahlosti:

1. PAN – personal area network
2. LAN – local area network – v rámci jednej budovy/poschodia
3. MAN – metropolitan area network – sieť v rámci mesta
4. WAN – wide area network – v rámci kontinentu

☺☻♥♦♣♠•◘○◙♂♀♪♫☼►•↕‼

## 10. Aplikácie

Aplikácia alebo používateľský aplikačný program vo výpočtovej technike a v informatike je počítačový program pomáhajúci používateľovi pri uskutočňovaní činnosti určitého konkrétneho typu, napríklad pri manipulácii s textami (textový procesor), číslami, grafikou a pod. Aplikácie môžu byť združené do aplikačných balíkov napr. kancelárskych ako sú Microsoft Office alebo LibreOffice.

### Proces

Proces je v informatike názov pre spustenú inštanciu počítačového programu. Proces je v operačnej pamäti počítača v podobe sledu strojových inštrukcií vykonávaných procesorom. Obsahuje nielen kód vykonávaného programu, ale aj dynamicky sa meniace údaje, ktoré sa spracovávajú. Program môže na jednom, ale aj na viac počítačoch bežať v podobe jedného či viacerých procesov s rôznymi dátami (napríklad viackrát spustený webový prehliadač zobrazujúci rôzne stránky).

### Webová aplikácia

Webová aplikácia je softvérová aplikácia, ktorá sa vykonáva na webovom prehliadači a je prístupná cez internet. Tieto aplikácie môžu byť interaktívne a poskytovať rôzne funkcie a služby, ako napríklad online nakupovanie, sociálne siete, online bankovníctvo a mnoho ďalších. Webové aplikácie sú často vytvorené pomocou kombinácie programovacích jazykov ako HTML, CSS a JavaScript. Sú veľmi populárne kvôli svojej dostupnosti a možnosti prístupu z rôznych zariadení s pripojením na internet. Výhody: šetrenie RAM, automatické updaty. Nevýhody: pripojenie na internet

## 11. Internet

### Komunikácia na internete

1. **interaktívna** - keď si užívatelia vymieňajú informácie (či už textové, grafické, zvukové, alebo video) v reálnom čase. Teda ON-LINE. Okamžite reagujú jeden na druhého.
2. **neinteraktívna -** kedy užívatelia nemôžu okamžite reagovať. Teda informácie, ktoré sú vyslané jednou osobou sa k adresátovi dostanú po istom čase a ten na ne reaguje (ak reaguje) s istým časovým odstupom. Za neinteraktívnu komunikáciu považujeme posielanie informácií prostredníctvom e-mailu, odkazovej schránky, SMS

### Poštový klient

v informatike názov pre samostatný počítačový program, ktorý sa používa na prijímanie, odosielanie a správu elektronickej pošty (e-mailu).

### DNS (Domain Name System)

je systém, ktorý prekladá prehliadačom názvy domén (napr. moodle.gvoza.sk) na IP adresy cieľových serverov (napr. 212.85.96.183). Keď prehliadač prijme preklad názvu domény, dochádza k prepojeniu a otvára sa určená internetová stránka.

### Poštový server

programy, ktoré sa starajú o doručovanie, distribúciu správ príjemcovi.

### SMTP

je skratka pre Simple Mail Transfer Protocol. Je to protokol, ktorý zabezpečuje odosielanie e‑mailových správ. Keďže protokol SMTP riadi komunikáciu pri odosielaní e‑mailov, tieto správy prechádzajú cez internet a odosielajú sa z poštových serverov. Každý takýto poštový server má svoje meno, preto je potrebné nastaviť názov servera (SMTP) pre odchádzajúcu poštu vo vašich e‑mailových klientoch.

### www

je názov pre systém zobrazovania, ukladania a odkazovania na dokumenty na internete. Webové stránky sa prezerajú pomocou webového prehliadača, ukladajú sa na webových serveroch a spájajú sa pomocou hypertextových odkazov zapísaných vo forme adries URL. Webové stránky sa opisujú pomocou jazyka HTML a na ich prenos medzi počítačmi sa používa protokol HTTP.

### POP3

POP3 (Post Office Protocol 3) poskytuje pripojenie k serverom prichádzajúcej pošty. POP však po pripojení k serveru sťahuje poštu do vášho počítača, teda e‑mailového klienta (Thunderbird, Outlook atď.). Tento protokol má veľkú nevýhodu v tom, že sťahuje celý obsah vašej poštovej schránky vrátane nevyžiadanej pošty alebo spamu.

### TCP/IP

je súbor protokolov na komunikáciu v počítačových sieťach používaných v celosvetovom internete. Jej názov je odvodený od dvoch najdôležitejších protokolov: internetový protokol (IP) je protokol sieťovej vrstvy, ktorý umožňuje komunikáciu medzi dvoma uzlami (počítačmi) v prepojenej sieti a protokol riadenia prenosu ( TCP) je protokol transportnej vrstvy, ktorý zabezpečuje spoľahlivý obojsmerný prenos údajov medzi aplikáciami.

### HTTP

znamená HyperText Transfer Protocol, je protokol používaný na komunikáciu medzi webovými prehliadačmi a webovými servermi. HTTP je komunikačný protokol, ktorý sa používa na prenos dát a informácií medzi webovými prehliadačmi a webovými servermi, na ktorých sú umiestnené webové stránky. Protokol je založený na bezstavovom modeli, čo znamená, že každá požiadavka od prehliadača je nezávislá a neuchováva si informácie o predchádzajúcich požiadavkách. HTTP je kľúčovým protokolom, ktorý umožňuje správne zobrazenie a prenos webových stránok. Keď užívateľ zadá adresu (URL) do prehliadača alebo klikne na odkaz, prehliadač vytvára HTTP požiadavku na príslušný webový server, ktorý potom posiela odpoveď s požadovanou stránkou alebo dátami.

### HTML

je hypertextový značkovací jazyk (z angl. hypertext markup language), s ktorým môžete tvoriť webstránky a dokumenty. Ide o kombináciu normálneho textu a značiek.

### IP

Základným protokolom sieťovej vrstvy a aj celého internetu je IP (Internet Protocol), ktorý funguje na základe tzv. IP adries. Tu využívajú všetky počítače či iné zariadenia s aktívnym prístupom do siete. Práve cez túto adresu sieťové protokoly určujú, do ktorého zariadenia majú doručiť určité dáta. IP protokol tak na základe IP adries vysiela tzv. datagramy obsiahnuté v ich záhlaví a poskytuje vyšším vrstvám sieťovú službu bez spojenia. Datagramy putujú sieťou nezávisle na sebe a sami tak nezaisťujú poradie ani spoľahlivosť doručenia. To zaisťujú až vyššie vrstvy, ako špecifické aplikácie alebo protokoly transportnej vrstvy.

### FTP

File Transport Protocol je označenie pre protokol pochádzajúci už zo začiatku 70. rokov, ktorý sa využíva k prenosu dát medzi dvomi počítačmi nepripojených na jednej sieti (napríklad vo firme), ale iba k internetu kdekoľvek na svete. Pre prácu s FTP je potrebné mať program (FTP klient), ktorý vám umožní rôzne operácie so súbormi a adresármi, ako napr. kopírovanie, premenovanie, nahrávanie dát na server a ich sťahovanie do vášho počítača.

### TELNET

Telnet je program spúšťaný z príkazového riadku (Windows, Linux...) slúžiaci k spojeniu počítačov v sieti TCP/IP.

### PING

je typ paketu v počítačovej sieti, ktorý sa používa na kontrolu, či je počítač, server, na ktorý sa chceme v sieti pripojiť k dispozícii alebo nie.

### TCP

Protokol TCP je najpoužívanejším transportným protokolom na internete. Na rozdiel od protokolu UDP realizuje potvrdzovaný prenos dát medzi soketmi. To znamená, že odoslané dáta z jedného soketu sa dostanú všetky a v rovnakom poradí do druhého soketu. Nakoľko aj protokol TCP využíva nespoľahlivý prenos dát nižších vrstiev (pakety sa môžu stratiť alebo prísť v inom poradí) musí zavádzať mechanizmy na overovanie toho, či segmenty došli všetky a nepoškodené. V prípade, že nie, tak musí vynútiť ich opätovné zaslanie. Tomuto princípu je podriadený takmer celý návrh protokolu.

### UDP

je tzv. "nespoľahlivý" protokol z balíka internetových protokolov. UDP protokol prenáša datagramy medzi počítačmi v sieti, ale na rozdiel od TCP nezaručuje, že prenášaný paket sa nestratí, že sa nezmení poradie paketov, ani že sa niektorý paket nedoručí viackrát. Vďaka tomu je UDP pre ľahké a časovo citlivé účely rýchlejší a efektívnejší.

### e-mailová adresa

je vaša poštová adresa, odkiaľ posielate a kam prijímate e-mailové správy.

### Doménová adresa

je jedinečná adresa na internete, ktorá môže odkazovať na nejaký web alebo webovú službu. Nahrádza IP adresu. Napríklad namiesto zapamätania si IP adresy: 46.229.238.141 si stačí len zapamätať [www.gvoza.sk](http://www.gvoza.sk) čo je určite jednoduchšie.

### IP adresa

IP adresa je logický číselný identifikátor (napr. 207.142.131.205) fyzického sieťového rozhrania daného uzla (najčastejšie počítača) v sieti, ktorý komunikuje s ostatnými uzlami prostredníctvom protokolu IP.

### Doména najvyššej úrovne

Doména najvyššej úrovne (TLD) je posledný segment doménového mena, ktorý nasleduje za poslednou bodkou v internetovej adrese. TLD rozdeľujú webové stránky do rôznych skupín na základe ich účelu alebo geografickej polohy.

### Internet

Internet je globálna sieť prepojených počítačových sietí, počítačov a iných zariadení. Umožňuje výmenu informácií, komunikáciu a zdieľanie zdrojov ako sú multimédiá a dáta. Slúži ako prenosové médium pre rôzne informácie a služby ako napr. elektronická pošta, chat a systém vzájomne prepojených webstránok a dokumentov World Wide Webu (WWW).

### Intranet

Intranet je súkromná sieť počítačov, ktorá je určená iba pre interné potreby spoločnosti.

### Možnosti pripojenia, poskytovatelia internetových služieb

**DSL** - využíva k vysokorýchlostnému pripojeniu na internet tiež pevnú telefónnu linku, pre pripojenie je potrebný modem.

**bezdrôtové lokálne siete Wi-Fi** - prepojené zariadenia komunikujú prostredníctvom rádiového signálu.

**satelitné pripojenie** - využívané je na veľké vzdialenosti, signál je dostupný všade, jeho zriadenie je však mimoriadne finančne nákladné. Charakteristická je dlhá doba odozvy.

**Internet prostredníctvom rozvodov káblovej televízie** - pre pripojenie k internetu sa využíva rozvod káblovej televízie.

**Optický internet** - signál je vedený prostredníctvom optického kábla, teda pomocou svetla. Pri kladení optických káblov je nutné dodržať maximálny povolený polomer ohybu. Vo veľkých mestách sa stáva štandardom, jeho rýchlosti sa pohybujú v desiatkach Mbit/s

## 12. Závislosť na internete, anonymita, zneužitie

### Počítačová kriminalita

Počítačová kriminalita sú trestné činy zamerané proti počítačom ako aj trestné činy páchané pomocou počítača.

### WAREZ

Termín počítačového slangu označujúci autorské diela, s ktorými sa zaobchádza v rozpore s autorským právom.

### POČÍTAČOVÉ PIRÁTSTVO

Neoprávnené nakladanie s počítačovými programami takým spôsobom, ktorý prináleží len autorovi.

### Hacker

**hacking** je neoprávnené vnikanie do cudzích systémov, najčastejšie v prostredí počítačových sietí

### Cracker

**crack** – upravená aplikácia alebo malý program, ktorý po inštalácii pôvodnej aplikácie nahradí súbor zabezpečujúci ochranu software

**cracking** – nepovolený prienik do cudzieho počítača či databázy

## 14. Malvér

Je všeobecné označenie škodlivého softvéru (malicious software).

### Ransomvér

Jedným z najčastejších typov malvéru s vysokou mierou úspešnosti je ransomvér. Tento typ malvéru sa nainštaluje do počítača obete, zašifruje jeho súbory a za ich obnovenie žiada výkupné (zvyčajne v podobe bitcoinu).

### Trójske kone

Trójske kone sa vydávajú za neškodné aplikácie, pričom používateľa podvodom prinútia stiahnuť si ich a používať ich. Po ich spustení môžu odcudziť osobné údaje, poškodiť zariadenie, sledovať aktivity alebo dokonca zariadenie napadnúť.

### Vírusy

Vírus zvyčajne dostanete ako prílohu k e-mailu, ktorá uchováva údajovú časť vírusu alebo škodlivú časť malvéru. Hneď ako obeť otvorí súbor, vírus nakazí zariadenie.

### Spyware

Spyware je program, ktorý sa do počítača nainštaluje zvyčajne bez vášho vedomia, pričom sleduje a prenáša osobné údaje, aktivitu prehliadania webu či ďalšie údaje jeho používateľovi. Spyware umožňuje svojim používateľom sledovať všetky formy komunikácie v cieľovom zariadení.

### PREVENCIA

1. pasívna ochrana
2. nepoužívať nelegálny software, nesťahovať ho z neznámych zdrojov
3. vyvarovať sa vkladaní rôznych médií
   * CD
   * DVD
   * FLASH DISK
4. zdieľať priečinky minimálne
5. neotvárať prílohy s neznámych zdrojov
6. nenavštevovať stránky s pochybným obsahom
7. pravidelné zálohovanie počítača
8. aktívna ochrana
   * používanie antivírusového programu (program, ktorý dokáže odhaliť vírus pri pokuse o infikovanie systému alebo vyliečiť už napadnutý systém)

### HOAX

Je varovná, poplašná, ale hlavne falošná správa varujúca pred neexistujúcim nebezpečenstvom, prosiaca o pomoc, ponúkajúca ľahký zárobok a podobne.

### ADWARE

Je software zobrazujúci reklamu, jeho súčasťou je často spyware.

### SPAM

Je nevyžiadaná správa, ktorej účelom je zvyčajne šírenie reklám dosť pochybnej kvality.

## 15. Šifrovanie

### Šifrovanie

Šifrovanie vo všeobecnosti znamená zmenu obsahu informácie (textu) na skupinu nezrozumiteľných znakov, ktorá je pre neoprávnenú osobu nečitateľná bez znalosti šifrovacieho kľúča.

### Kód

pravidlo pre prevod informácie (napríklad listu, slova alebo frázy) na inú formu alebo reprezentáciu, nie nevyhnutne rovnakého typu. Vo všeobecnosti je kód zobrazenie, ktoré každému znaku alebo postupnosti znakov daného súboru znakov (vzorov) jednoznačne priradí znak alebo postupnosť znakov (obrazov) z iného súboru znakov

### Symetrické šifry

Predstavujú kategóriu šifier, v ktorých sú šifrovacie kľúče pre šifrovanie a dešifrovanie rovnaké. Tieto šifry vyžadujú, aby sa príjemca aj odosielateľ vopred dohodli na kľúči, ktorý budú používať a potom ho tajili. Ak sa ten istý kľúč používa dlhšiu dobu, vzniká nebezpečenstvo jeho prezradenia alebo v prípade mnohonásobného používania i dešifrovania, a preto sa kľúče často obmieňajú.

### Substitučné šifry

Princíp substitučných šifier je v tom že každé písmeno nezašifrovanej správy sa zmení na iné písmeno.

### Transpozičné šifry

Substitučné šifry sú založené na nahradzovaní písmen inými písmenami, transpozícia je poprehadzovanie písmen. Písmená sa nemenia len sa zmení ich pozícia v texte. Ako daná transpozícia prebieha závisí od šifrovacieho algoritmu. Existuje veľké množstvo jednoduchých ale aj zložitejších transpozičných šifier.

### Polyalfabetické šifry

Sú tvorené viacerými jednoduchými šiframi, ktoré spolu vytvoria veľmi silnú šifru.

### Asymetrické šifry

Sú založené na myšlienke používania dvojice kľúčov : verejného a súkromného. Pomocou jedného z nich sa správa zašifruje, prostredníctvom druhého dešifruje. Príjemca správy nemusí poznať kľúč, prostredníctvom ktorého boli údaje zašifrované a odosielateľ nemusí poznať kľúč, ktorý správu dešifruje. Majiteľ svoj verejný kľúč poskytne všetkým, s ktorými chce komunikovať a oni správy prostredníctvom neho zašifrujú. Dešifrovať takto zašifrovanú správu možno už len pomocou súkromného kľúča, ktorého jediným vlastníkom je prijímateľ správy. Sila tohto typu šifrovania spočíva v tom, že komunikujúci svoje kľúče nemusia poznať a z toho dôvodu ich nemôžu poskytnúť nikomu ďalšiemu.

### Dôvody šifrovania informácii

* Ochrana citlivých dát
* Bezpečnosť
* Pravosť dokumentov – elektronický podpis

### Digitálny podpis

je všeobecnejší variant elektronického podpisu, používaný len na overenie integrity údajov - nepozmenenosť. Neumožňuje overiť ich autentifikáciu - pôvod. Za konkrétny príklad digitálneho podpisu možno považovať dôveryhodné overenie hašu vygenerovaného z údajov. Digitálne podpísaný dokument predstavuje: po digitalizácii dokumentu, sa vypočíta hašovaciou funkciou krátky haš, ktorý sa dôveryhodne uchová (prenesie) oddelene od dokumentu a v budúcnosti (u protistrany) zaručuje, že dokument nebol v čase (pri prenose) nijak pozmenený. Zaručenie takéhoto digitálneho podpisu úzko súvisí s bezpečnosťou použitej hašovacej funkcie. Funkciu nemožno považovať za bezpečnú, nezaručuje viac digitálny podpis, ak boli zverejnené postupy hľadania kolízii tejto hašovacej funkcie.

### HASH

Transformácia vstupu na reťazec pevnej dĺžky. V súčasnosti 256 bitov. **Vlastnosti**: ľubovoľná dĺžka vstupu, pevná dĺžka výstupu, jednosmerný algoritmus (nie je inverzná funkcia),

Využitie: uchovávanie hesiel, digitálny podpis, overenie integrity. Toto zobrazenie väčšej množiny vstupov, do menšej množiny výstupov, nie je prosté. Preto určite existujú dva rôzne vstupy, ktoré dávajú rovnaký výstup. Týmto konkrétnym rôznym dátam sa hovorí kolízie hašovacích funkcií. Bežné hašovacie funkcie, ktoré nemožno považovať za bezpečné by mali spĺňať:

**Rýchlosť transformácie** – funkcia rýchlo spočíta zo vstupu x výstup

**Rozloženie výstupov** – funkcia musí distribuovať výstupy rovnomerne v celom obore hodnôt, teda produkuje málo kolízii.

**Lavínovitosť** – vytvorený hash musí natoľko závisieť na každom bite vstupu, že aj jeho malá zmena rapídne ovplyvní výstup.