

Úvod do informatiky

Informácia - vyjadruje význam prisudzovaný údajom. Odstraňuje vždy určitú mieru nevedomosti v poznaní u príjemcu.

Znalosti - sú vytvárané z informácií uvádzaných do súvislostí, ktoré nám umožňujú predvídať určité javy, sú teda predpokladom na správne jednanie a rozhodovanie.

Informatika - je vedná disciplína, ktorá sa zaoberá informačným procesom t.j. zberom, prenosom, spracovaním a archiváciou informácií.

Zber – je zisťovanie a zaznamenanie údajov na nosič

Prenos- prenesenie údajov z miesta zberu na miesto spracovania. Môže byť ručný, počítačovou sieťou, internetom a pod.

Spracovanie – je premena údajov na informácie pomocou aritmetických, triediacich a logických operácií

Archivácia – je uchovanie informácií na vhodnom nosiči

Počítač - z tohto pohľadu je technickým prostriedkom, ktorý slúži na realizáciu týchto operácií v informačnom procese.

Pozn.:

1. *Pojem informácia je odvodený od latinského slova „informare“, teda formovať mienku.*
2. *Pojem informatika vznikol v šesťdesiatych rokoch vo Francúzsku spojením slov „information“ (informácia) a „automatique“ (automatický). Nové slovo „informatique“ (informatika) sa tak stalo názvom pre spracovanie informácií pomocou automaticky pracujúcich strojov (počítačov)*
3. *Dnes vás hlavne reklama a médiá často nútia rozhodovať sa na základe pocitov. Pokiaľ sa naučíte svoje rozhodnutia racionálne a logicky zdôvodňovať na základe objektívnych informácií, budete úspešnejší a spokojnejší aj v živote.*

Úloha:

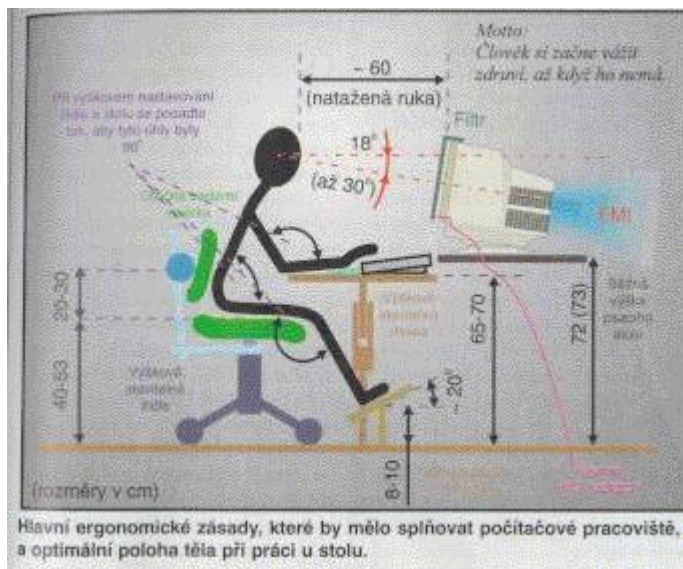
1. *Zistite priemer známok z informatiky u žiakov vo vašej triede*
2. *Zistite študenta s najlepším a najhorším priemerom*
3. *Pri práci si uvedomte jednotlivé operácie s informáciami*
 - a. *zber* – zistenie známok z informatiky a zápis na papier, cd a pod.
 - b. *prenos* – na miesto spracovania, kde je počítač, kalkulátor a pod.
 - c. *spracovanie*
 - *sčítanie známok jednotlivých študentov*
 - *vydelenie súčtu počtom známok študenta*
 - *triedenie podľa priemeru na zistenie najmenej a najväčšej hodnoty*
 - d. *archivácia*- uchovanie výsledkov na nosič napr. papier, cd, USB a pod.

Ergonómia počítačového pracoviska

Ergonómia je vedecká disciplína, ktorá sa zaoberá prispôbovaním pracovného prostredia potrebám človeka.

Používanie počítačov prináša so sebou nové zdravotné problémy a riziká. Sú to:

1. Zvýšené nároky na zrak
2. Statická záťaž pohybového aparátu (prsty, chrbtica, krk a pod)
3. Psychická záťaž, stres a mentálne zmeny
4. Elektromagnetické žiarenie a pod.



Pri vytváraní počítačového pracoviska by mali byť dodržané tieto ergonomické zásady:

1. Stolička

- otočná
- nastaviteľná výška a sklon
- so stabilným alebo pohyblivým podstavcom

2. Stôl

- veľkosť približne 1,6 x 0,8 m
- spracované doklady po ľavej strane od klávesnice

3. Obrazovka

- umiestnená kolmo na okno tak, aby na nej neboli žiadne svetelné odrazy
- horný okraj monitora vo výške očí
- vzdialenosť monitora na dĺžku ruky, poloha meniteľná
- elektromagnetické žiarenie u CRT monitorov je až na 90 % zachytávané filtermi zabudovanými priamo v skle
- nemali by sme sa pohybovať v tesnej blízkosti bočných stien a zadnej časti, i keď vo vzdialenosti 50 cm je elektromagnetické žiarenie nulové

4. Rytmus práce

- bez prestávky nepracovať dlhšie ako 1 hodinu
- potom klesá schopnosť koncentrácie a zvyšuje sa počet chybných úkonov

5. Klávesnica

- voľne posunovateľná
- sklon asi 15 °, pretože to ovplyvňuje postavenie ruky
- v takej výške, aby ruky zvierali približne 90 ° uhol

6. Pri práci s počítačom je

- povolená hlučnosť do 56 decibelov
- teplota 20-25 ° C
- voľná podlahová plocha 12-15 m² vrátane nábytku
- osvetlenie miestnosti 500 Luxov
- relatívna vlhkosť vzduchu 50-56 %

Vo Švédsku pri výskume vykonanom na 500 pracovníkoch používajúcich pri práci počítač, boli zistené zdravotné problémy

s očami	75 %
s chrbticou a ramenami	25 %
s hlavou a krkom	35 %
s lakt'ami a zápästím	25 %
s nohami	15 %

Tieto zdravotné problémy sa prejavovali už po dvoch rokoch práce s počítačom!

S cieľom minimalizovať tieto problémy, boli vydané medzinárodné štandardy **ISO 9241**, ktoré spresňujú ergonomické požiadavky na pracoviskách s počítačom. Pre krajiny EÚ bola na tieto účely vydaná smernica **90/270/EC** z roku 1990

Súčasný pracovník je charakterizovaný ako video unit operátor (pracovník pri obrazovke).

Poznámka:

Táto téma bola vypracovaná v súlade s nariadením vlády SR č. 247/2001 o minimálnych bezpečnostných a zdravotných požiadavkách pri práci so zobrazovacími jednotkami, podľa materiálov Dublinskej nariadenia a nemeckých metodických materiálov.

Úloha:

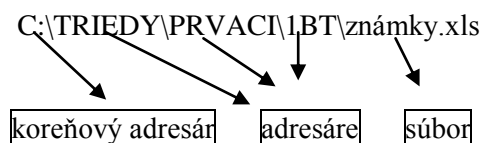
1. Pomocou internetového prehliadača zistíte a zapíšete do zošita:
 - stručný obsah európskej smernice 90/270/EC
 - význam pojmov TCO95, TCO99 alebo TCO03 uvádzaných na monitoroch
 - čo najviac škodí počítačom?
2. Posúďte svoje počítačové pracovisko v škole z hľadiska ergonomických požiadaviek a u každého bodu zapíšete do zošita, či je splnené alebo nie
3. Ďalšie informácie nájdete na webovej adrese
http://di.ics.upjs.sk/informatika_na_zs_ss/studijny_material/it_spolocnost/ergonomia/ergonomia.htm

Štruktúra uloženia údajov v počítači

Všetky údaje, ktoré spracováva počítač sú vo forme súborov (file). Názov súboru sa skladá z mena, bodky a typovej prípony, ktorá určuje formát súboru. Prípona je definovaná pri vytvorení súboru implicitne alebo ju vytvorí užívateľ.

Pre uloženie súborov do počítača platia tieto zásady:

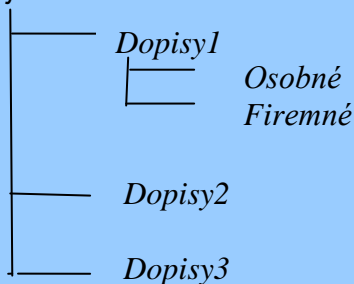
1. Súbory sa umiestňujú do **adresárov** (priečinkov)
2. Štruktúra adresárov tvorí tzv. **strom** (tree)
3. Súbory sú prístupné až po zadaní **cesty** (path)



Úloha:

1. Vytvorte na pracovnej ploche priečinky **Moje, Dopisy1, Osobné, Firemné, Dopisy2 a Dopisy3** s nižšie uvedenou stromovou štruktúrou
2. Vo Word Pade vytvorte súbor vo formáte **ÚlohyB.txt**, napíšte tam svoje meno, priezvisko a uložte ho cez **Súbor- Uložiť ako** do priečinku **Osobné**
3. Prácu s programom Word Pad ukončíte príkazom **Súbor -Skončiť** a znovu otvorte svoj súbor **ÚlohyB.txt** cez **Súbor - Otvoriť**
4. Prácu s programom Word Pad ukončíte a priečinky odstráňte z pracovnej plochy

Moje



Textové, grafické a multimediálne informácie.

1. **Textové**- vytvárajú
 - a. textové editory –Word Pad, Word (formáty **.doc, .txt, .rtf** a pod)
 - Acrobat Reader (formát **.pdf**) zabezpečuje rovnaké zobrazenie textu na každom počítači, ale nedá sa upravovať.
 - b. skenery – umožňujú vytvoriť rôzne formáty naskenovaného textu
2. **Grafické** – obrázky, fotografie, schémy. Môžu byť
 - a. **rastrové** – bod obrázka určujú súradnice. Môžeme ich vytvoriť napr.
 - programom Skicár vo formáte napr. **.bmp, .jpeg, .gif, .tiff**
 - digitálnym fotoaparátom vo formáte napr. **.pcf**
 - skenerom vo formáte napríklad **.xmp**

Zmena veľkosti obrázka sa prejaví na jeho kvalite.

- b. **vektorové** – bod obrázka určujú dve krivky. Vektorové obrázky môžeme vyhotoviť napr.
 - grafickým programom Corel Draw vo formáte **.cdr**
 - upraviť fotografie napr. programom Adobe Photoshop vo formáte **.psd**, Corel Photo Point vo formáte **.cpt**

Zmena veľkosti obrázka nemá vplyv na jeho kvalitu.

Konverzia z vektorového na rastrový obrázok je možná, opačne však nie.

3. **Multimediálne**(audiovizuálne) – zvuk, video. Môžeme ich vytvoriť pomocou mikrofónu, syntetizátora alebo videokamerou napr. vo formáte **.wav, .awi, .svg, .ogg**

Úloha:

1. V programe Skicár systému Windows nakreslite ľubovoľný obrázok a uložte ho vo formáte **.jpeg**
2. Otvorte program Corel Draw a príkazom **Súbor –importovať** ho importujte, **zväčšite jeho rozmery** a uložte ho príkazom **Súbor – Uložiť ako** vo formáte **.cdr**
3. **Zistite v oboch programoch , či zväčšením obrázka znížila sa jeho kvalita**

Komprimácia informácií.

Vysoké nároky multimediálnych informácií na technické parametre počítačov spôsobili nutnosť ich komprimovať (stlačiť, zmenšiť ich objem).



1. Textové informácie – komprimujeme programom napr. WinRar do formátov **.rar, .zip**
2. Grafické informácie komprimujeme do formátov
 - a. stratových – vynechávajú sa určité informácie, ktoré však človek nevníma, napr. **.jpeg** (fotografie)
 - b. bezstratové – konverzia všetkých informácií bez straty, do formátov napr. **.gif, .spg, .png**
3. Multimediálne informácie komprimujeme napr., zvukové z formátu **.wav** do formátu **.mp3, .wma** a pod. Video z formátu **.avi** komprimujeme do formátu **.mpeg4, .DivX, .wmv** a pod.

Programy, ktoré umožňujú konverziu multimediálnych informácií nazývame kodeky. V súčasnom období sme svedkami splývania spotrebnej elektroniky s výpočtovou technikou


Formát **GIF** rovnako ako formáty **PNG** a **JPEG** sa používajú pre **WWW** grafiku na **Internet**.

Formáty audiovizuálnych informácií	
Obrázky	APNG • BMP • GIF • HDP • JPEG • JPEG 2000 • MNG • PCX • PNG • SVG • TIFF • WBMP • XPM
Video	MPEG-1 • MPEG-2 • MPEG-4 ASP • H.264 (MPEG-4 AVC) • HuffYUV • RealVideo • Theora • Dirac • WMV
Zvuk	AAC • Apple Lossless • AC-3 • AMR • ATRAC • FLAC • G.711 • G.729 • MP3 • MOD • Speex • Vorbis • TAK • WAV • WMA • Musepack

Úloha:

1. **Použitím programu WINRAR skomprimujte súbory podľa tohto postupu:**
 - a. prejdite do priečinka, ktorý obsahuje súbory na komprimáciu (archivovanie, pakovanie)
 - b. označte súbory, ktoré chcete archivovať
 - c. klik na tlačidlo **ODHADNÚŤ**  , ktoré zistí účinnosť kompresie
 - d. klik na tlačidlo **PRIDAŤ**  , zvolte formát archívu napr. **RAR** alebo **ZIP**, metódu kompresie, prípadne iné parametre
 - e. klik na **OK**, pričom proces archivácie sa zobrazuje i graficky. Archivovaný súbor je automaticky doplnený o príponu **.arj** alebo **.zip**

2. Vytvorte samorozbalovací archív podľa tohto postupu:

- na karte **OBEČNÉ** môžete vybrať „**ARCHÍV SFX**“, ktorý vytvorí archívny súbor s príponou **.exe**.
- existujúci archív s príponou **.rar** viete previesť na samorozbalovací tak, že ho najprv označíte, potom klik na **PRIDAŤ**  a označíte voľbu „**VYTVORIŤ SFX ARCHÍV**“ a **OK**
- samorozbalovací archív použijete tak, že ho najprv prekopírujete na miesto extrakcie (dekomprimácie, rozbalenia) a potom ho spustíte dvojklikom.

Poznámka.: Na extrakciu XFS archívu nie je potrebný koprímačný program WINRAR.

3. Extrakcia archívnych súborov:

- označíte archívny súbor s príponou **.rar** a klik na tlačidlo **EXTRAHOVAŤ DO**
- nastavíte cieľovú cestu, kam chcete súboru rozbaľiť, prípadne vytvoríte priečinok a **OK**.

4. Ďalšie informácie nájdete na internetovej adrese <http://cs.wikipedia.org/wiki/Kodek>

Číselné sústavy

Počítač pracuje s číslicami, textom a inými znakmi, ktoré musí zakódovať (previesť) do tvaru, ktorému bude rozumieť. Je to kombinácia núl a jednotiek dvojkovej (binárnej) sústavy, ktorá zodpovedá dvom fyzikálnym stavom integrovaných obvodov (vodivý, nevodivý). Je základom na digitalizáciu analógových informácií.

Údajom, ktoré sú uložené v počítači ako kombinácia núl a jednotiek hovoríme bity. Skupina 8 bitov tvorí 1 Byt (1 znak). V súčasnosti vieme zakódovať kódom ASCII pomocou 8 bitov 256 znakov (2^8). Na zakódovanie väčšieho počtu znakov je to ale málo, preto novší kód UNICODE používa na vyjadrenie 1 znaku 16 bitov, teda umožňuje zakódovať až 65 536 znakov (2^{16}).

Byte sa stal jednotkou pre udávanie kapacity pamäte počítačov, veľkosti súborov a pod.. Dnes používame jeho násobky napr. KB, MB, GB, TB.

1 KB=1 024 B

1 MB=1 024 KB

1 GB=1 024 MB atď.

Pre programátora je užitočné, aby vedel používať okrem desiatkovej aj dvojkovú a šestnástkovú sústavu.

- Dvojková sústava obsahuje 2 znaky 0, 1
- Desiatková sústava obsahuje 10 znakov 0,1, 2 . . 9
- Šestnástková sústava obsahuje 16 znakov

0,1,2 . . 9,	A	B	C	D	E	F
	10	11	12	13	14	15

Prevody medzi číselnými sústavami:

$$\begin{aligned} 10010110_2 &= 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 \\ &= 128 \qquad \qquad +16 \qquad \qquad +4 \qquad +2 \\ &= 150_{10} \end{aligned}$$

$$\begin{aligned} A8EC_{16} &= 10 \cdot 16^3 + 8 \cdot 16^2 + 14 \cdot 16^1 + 12 \cdot 16^0 \\ &= 40\,960 + 2\,048 + 224 + 12 \\ &= 43\,244_{10} \end{aligned}$$

$$\begin{array}{r} A8EC_{16} = 1010/1000/1110/1100_2 \end{array} \begin{array}{r} \begin{array}{c} \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ \text{---} \text{---} \text{---} \text{---} \\ \text{---} \text{---} \text{---} \text{---} \\ \text{---} \text{---} \text{---} \text{---} \\ \text{---} \text{---} \text{---} \text{---} \end{array} \begin{array}{l} A \\ 8 \\ E \\ C \end{array} \end{array} \begin{array}{r} \begin{array}{r} 8 \ 4 \ 2 \ 1 \\ \hline 1 \ 0 \ 1 \ 0 \\ 1 \ 0 \ 0 \ 0 \\ 1 \ 1 \ 1 \ 0 \\ 1 \ 1 \ 0 \ 0 \end{array} \end{array} \quad (\text{váhy})$$

$$0010/1010/1110_2 = 2AE_{16}$$

$$43124_{10} = A874_{16}$$

zvyšok

$$\begin{array}{l} 43\ 124 : 16 = 2\ 695 \\ 2\ 695 : 16 = 168 \\ 168 : 16 = 10 \\ 10 : 16 = 0 \end{array}$$

4
7
8
10

$$2\ 634_{10} = 1010/0100/1010_2$$

$$\begin{array}{l} 2\ 634 : 2 = 1\ 317 \\ 1\ 317 : 2 = 658 \\ 658 : 2 = 329 \\ 329 : 2 = 164 \\ 164 : 2 = 82 \\ 82 : 2 = 41 \\ 41 : 2 = 20 \\ 20 : 2 = 10 \\ 10 : 2 = 5 \\ 5 : 2 = 2 \\ 2 : 2 = 1 \\ 1 : 2 = 0 \end{array}$$

zvyšok

0
1
0
1
0
0
1
0
0
1
0
1

Úloha:

1. Urobte prevody medzi číselnými sústavami:

$$\begin{array}{l} 34\ 124_{10} = \quad \quad 16 \\ 279_{10} = \quad \quad 2 \\ 100010111_2 = \quad 10 \end{array}$$

2. Skontrolujte správnosť prevodu medzi číselnými sústavami pomocou vedeckej kalkulačky systému Windows

Šifrovanie informácií

Kryptografia je vedná disciplína, ktorá sa zaoberá šifrovaním informácií. Cieľom šifrovania je utajovanie informácií a bezpečná komunikácia.

Na vytváranie šifier sa používajú šifrovacie programy alebo technické prostriedky.

Existuje:

1. **Symetrické šifrovanie** – algoritmus šifrovania je rovnaký ako pri dešifrovaní. Používa sa pri miestnom šifrovaní napríklad na disku počítača. Pre prenos údajov je menej vhodný, pretože je potrebné preniesť aj šifru. Existujú **posuvné** a **substitučné** symetrické šifry.

2. **Asymetrické šifrovanie** –používa sa na bezpečný prenos údajov a na komunikáciu. Používa sa verejný a súkromný kľúč. Tieto kľúče sú šifrovacím algoritmom zviazané (existuje vždy len jeden pár). To znamená, že správu zašifrovanú verejným kľúčom je možné dešifrovať len k nemu vytvoreným súkromným kľúčom. Postup je nasledovný:
- pomocou šifrovacieho programu sa vygenerujú (vytvoria) oba kľúče, verejný aj súkromný
 - súkromný kľúč sa bezpečne uchová napríklad na USB disk, jeho prístup sa chráni heslom.
 - verejný kľúč sa odošle všetkým odosielateľom dokumentu, od ktorých chceme obdržať zašifrovaný dokument
 - obdržaný dokument sa dešifruje príslušným súkromným kľúčom

Medzi najjednoduchšie symetrické šifry patria zámenny písmen (substitučné šifry). Šípka smerom dole ukazuje smer šifrovania a šípka smerom hore ukazuje smer dešifrovania.

pôvodná správa:	tajna sprava	pôvodná správa:
smer šifrovania ↓	kľúč: a b c d e f g h i j k l m n o p q r s t u v w x y z ↓ w k l c x y z f g h i j a b o p q r s t u v d e m n	↑ smer dešifrovania
	zašifrovaná správa	

Ďalšou možnosťou sú posuny v abecede (posuvné šifry). Predpokladajme, že budeme posúvať abecedu o štyri znaky (mimochodom toto je šifra, ktorú používal aj Julius Caesar).

pôvodná správa:	tajna sprava	pôvodná správa:
smer šifrovania ↓	kľúč: posuň písmená v abecede o 4 znaky	↑ smer dešifrovania
zašifrovaná správa	xenredwtveze	zašifrovaná správa

Úloha:

- Vytvorte jednoduchú posuvnú a substitučnú symetrickú šifru a zašifrujte pomocou nich svoje meno a priezvisko
- Zapíšte do zošita, v čom vidíte rozdiel medzi kódovaním a šifrovaním informácií
- Ďalšie informácie nájdete na internetovej adrese http://di.ics.upjs.sk/informatika_na_zs_ss/studijny_material/sifry/pgp/pgp1.htm