

BA (Hons) in Business Management
BA (Hons) in Business Management – Double degree
Bc. Ekonomika a management
2. ročník

Informatika pro ekonomy

(learning package)

Jiří Rybička

2011/2012



Autor tohoto studijního materiálu prohlašuje, že tento zpracoval v souladu s mezinárodními autorskými právy. Autor se zavazuje uhradit veškerou škodu vzniklou jejich případným porušením.

Informatika pro ekonomy (learning package) ©
doc. Ing. Jiří Rybicka, Dr.
rybicka@mendelu.cz

Obsah

1. Základní informace o modulu	4
1.1 Vyučující modulu	4
1.2 Cíl výuky v modulu	4
1.3 Struktura přednášek modulu	4
1.4 Hodnocení a jeho kritéria	5
1.4.1 Písemná práce (assignment), váha v celkovém hodnocení 50 %	5
1.4.2 Písemná zkouška	6
1.5 Doporučená studijní literatura	6
1.5.1 Základní studijní literatura	6
1.5.2 Rozšiřující literatura	6
1.5.3 Podpora pro zpracování assignmentu po formální a technické stránce	7
2. Doplnující studijní materiál	8
2.1 Úvod do počítačové grafiky	8
2.2 Datové formáty	15
2.3 Informace v počítači	21
2.4 Přenos dat, kódování	26
2.5 Zabezpečení informace	30
2.6 Komprimace a archivace dat	39
2.7 Internetové technologie	45
2.8 Databázové systémy	51
2.9 Informační systémy	58

1. Základní informace o modulu

1.1 Vyučující modulu

Jméno	Telefon	e-mail
VEDOUcí MODULU		
doc. Ing. Jiří Rybička, Dr.	545 132 223	rybicka@mendelu.cz

Jiří Rybička pracuje jako docent na Ústavu informatiky Provozně ekonomické fakulty Mendelovy univerzity v Brně a dlouhodobě se věnuje problematice výuky informatiky a informačních technologií, a to zejména u studentů neinformatických oborů. Vyučuje předměty Zpracování textů počítačem, Informatika pro ekonomy a Informatika v agrobyznysu. U studentů informatických oborů vyučuje předmět Programovací techniky. Podílí se rovněž na vývoji univerzitních informačních systémů nasazených v ostrém provozu na pěti univerzitách v ČR a na Slovensku. Je členem sdružení zabývajícím se kvalitní typografií, spolupracuje s některými nakladatelstvími jako realizátor knižní sazby.

1.2 Cíl výuky v modulu

Získání základního přehledu o principech funkce a možnostech využití moderních informačních a komunikačních technologií, zejména při aplikacích v podniku. Obsah je složen z okruhů, které na sebe logicky navazují a tvoří ucelený komplex pokrývající základní aplikační oblasti – kvantifikace informace, přenos dat, internetové technologie, problémy zabezpečení a ochrany dat, grafické systémy, databázové technologie a informační systémy podniku včetně základů jejich analýzy a uplatnění.

1.3 Struktura přednášek modulu

Téma číslo	Přednášená látka
1.	Zpracování grafické informace počítačem
	a) Princip uložení grafické informace
	b) Obrazové editory a jejich použití
2.	Ukládání dat v počítači
	a) Jak vypadají data v počítači
	b) Souborové formáty a jejich využití
	c) Úvod do teorie informace

Téma číslo	Přednášená látka
3.	Přenos dat, kódování
	a) Signál, komunikace, komunikační řetěz
	b) Kódování informací v praxi
4.	Zabezpečení a ochrana dat
	a) Zabezpečení informace při přenosu
	b) Počítačová kriminalita
	c) Komprimace a archivace údajů
5.	Technologie sítě Internet
	a) Základní pojmy
	b) Statické a dynamické webové dokumenty
	c) Aplikace webových technologií v praxi
6.	Databázové systémy
	a) Vznik a vývoj databázových systémů
	b) Relační databázový model
	c) Návrh datového modelu
	d) Implementace a aplikace databázových systémů v praxi
7.	Úvod do aplikace informačních systémů
	a) Základní pojmy z oblasti informačních systémů (IS)
	b) Rysy současné společnosti ve vztahu k IS
	c) Efektivnost při zavádění IS, náklady a přínosy

1.4 Hodnocení a jeho kritéria

1.4.1 Písemná práce (assignment), váha v celkovém hodnocení 50 %

Téma assignmentu je poměrně široké. Jeho hlavním smyslem je aplikace poznatků tohoto modulu v konkrétních praktických podmínkách podle individuálního výběru daného studenta.

Zadání assignmentu: Analýza programového vybavení v oblastech zmiňovaných v tomto modulu, jeho skutečné nebo možné využití ve zvoleném podniku a případný návrh na zlepšení. Příklady aplikačních oblastí: počítačová grafika, souborové formáty, konverze a kódování souborů při přenosech, kódování národních znaků a jeho řešení, komprimace a archivace dat, webové technologie a jejich aplikace, technologie databázových systémů, možnosti implementace informačních systémů.

Tématem assignmentu nemůže být technické řešení (výběr počítačů, tiskáren nebo jiných zařízení, návrh a řešení síťového propojení nebo napojení na internetovou síť apod.), tématem rovněž nemůže být analýza, projektování a realizace podnikových nebo jiných informačních systémů. Uvedená témata jsou součástí jiných modulů.

Práce musí obsahovat *popis současného stavu* aplikace zvoleného programového vybavení v podniku se zaujetím *vlastního stanoviska* nebo *vlastním komentářem*, s případným návrhem na úpravu, rozšíření nebo zavedení popisované aplikace.

Rozsah práce by se měl pohybovat mezi 7–10 stranami textu formátu A4, při písmu 12 bodů a běžném řádkování 14 až 15 bodů. Formální úprava musí odpovídat typografickým pravidlům, jazykovým pravidlům, ustanovením normy pro bibliografické citace ČSN ISO 690 (část 1 a část 2) a technickým požadavkům na zpracování (používání správně nastavených stylů apod.). Podrobné informace o zpracování odborných textů jsou prezentovány v rámci modulu Informační technologie, rovněž lze použít materiál Zpracování textů v programu Word vystavený na adrese

<http://akela.mendelu.cz/~rybicka/prez/zpract/odbprace/bibsword.rtf>

Kritéria hodnocení písemné práce

Kritérium	Váha
Schopnost shromáždit potřebné informace a fakta (jak z odborné literatury, tak i z reality zvoleného podniku), analyzovat a interpretovat je v duchu teorie daného modulu	30 %
Formulovat relevantní a srozumitelné závěry a doporučení , případně vlastní stanoviska k popisovaným problémům	30 %
Formální úprava práce včetně citací a dodržení stanoveného rozsahu	30 %
Schopnost argumentovat ve prospěch závěrů a doporučení	10 %

1.4.2 Písemná zkouška

Zkouška z modulu v celkové váze hodnocení 50% probíhá v elektronické formě. Předpokládá se znalost přednesené látky a schopnost uplatnit aktivní poznatky. Hodnocení testu a jeho formální a obsahové náležitosti se řídí vnitřními předpisy školy, Provozním řádem PC učebny a interními postupy. Obsahové požadavky zkoušky jsou v souladu s obsahovou náplní modulu a řídí se vnitřními předpisy a studijním a zkušebním řádem školy. Testové otázky jsou rozděleny do jednotlivých okruhů, z nichž každý může mít různé bodové hodnocení. Správně zodpovězené otázky jsou hodnoceny plus body, za špatně zodpovězenou otázku se odečítá vždy 1 bod. V případě, že otázka zůstane nezodpovězena, je hodnocena 0 body.

1.5 Doporučená studijní literatura

1.5.1 Základní studijní literatura

- RYBIČKA, J., TALANDOVÁ, P. *Informatika pro ekonomy*. Praha: Alfa publishing, 2009.

1.5.2 Rozšiřující literatura

- BASL, J. *Podnikové informační systémy*. 2. vyd. Praha: Grada, 2008.
- DOMES, M. *Tvorba internetových stránek pomocí HTML, CSS a JavaScriptu*. Brno: Computer Media, 2005.
- MURRAY, J. D., VANRYPER, W. *Encyklopedie grafických formátů*. Brno: Computer Press, 2005.
- POKORNÝ, J., HALAŠKA, I. *Databázové systémy*. Praha: Vydavatelství ČVUT, 2003.
- SATRAPA, P. *WWW pro čtenáře, autory a misionáře*. Praha: Neokortex, 2003.

- SINGH, S. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. 1. vyd. Praha: Dokořán, Argo, 2003.
- Příručky ke konkrétnímu programovému vybavení podle vlastního výběru.

1.5.3 Podpora pro zpracování assignmentu po formální a technické stránce

- RYBIČKA, J. *Základy zpracování textů*. Brno: Konvoj, 2000.
- RYBIČKA, J. *Zpracování textů v programu Word* [online]. Dostupné na <http://akela.mendelu.cz/~rybicka/prez/zpract/odbprace/bibsword.rtf>
- *ČSN ISO 690 – Bibliografické citace. Obsah, forma, struktura*. Praha: Český normalizační institut, 1997.

2. Doplnující studijní materiál

Podklady prezentací k přednáškám

2.1 Úvod do počítačové grafiky





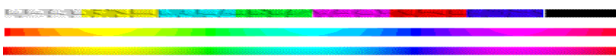
Barevná hloubka =

počet bitů potřebných na uložení barvy pixelu

- 1 pixel = barva/prázdnost
– monochromatický obraz, 1 pixel = 1 bit
- 1 pixel = určitá barva z palety
– obraz s paletou, 1 pixel = 2, 4, 8, 16 bitů
- 1 pixel = intenzita jedné barvy
– odstíny šedi, 1 pixel = 8 bitů
- 1 pixel = složení libovolné barvy
– pravé barvy (true color), 1 pixel = 24 bitů

Barvy a jejich reprezentace

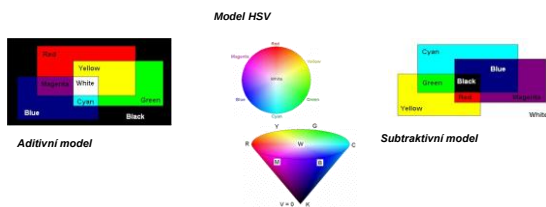
- vlnění v oblasti 10^8 MHz (barva odpovídá frekvenci)
- červená ($4,3 \times 10^8$ MHz)
- fialová ($7,5 \times 10^8$ MHz)
- nižší hodnoty — infračervené světlo
- vyšší — ultrafialové záření
- V rámci viditelné části spektra je člověk schopen rozlišit víc než 4×10^5 různých barev a jejich odstínů.



Barevné modely

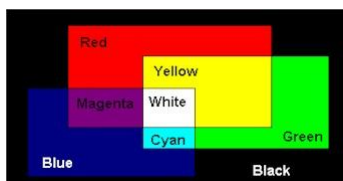
Barevný model odpovídá na tři otázky:

- Ze kterých základních barev se budou ostatní skládat?
- Jaký bude poměr jednotlivých základních barev?
- Jakým způsobem se budou základní barvy míchat?



Aditivní barevný model (typicky RGB)

- Barvy jsou vytvářeny přidáváním barvy do černé.
- Aditivní barevné prostředí nepotřebuje vnější světlo (barvy na monitoru).
- Používá se při ukládání do souborů.



Subtraktivní barevný model (typicky CMY)

- Základní barvy jsou odečítány od bílé, čím více odeberu, tím více se blíží černé.
- Subtraktivní prostředí je prostředí, které odráží světlo, a proto potřebuje vnější zdroj světla.
- Používá se v tiskárnách, plotrech, ve fotografii.
- CMY(K) (Cyan, Magenta, Yellow, black)



Ekvivalentní RGB, CMY a HSV hodnoty

barva	R G B	C M Y	HSV
červená	255, 0, 0	0, 255, 255	0°, 100%, 100%
žlutá	255, 255, 0	0, 0, 255	60°, 100%, 100%
zelená	0, 255, 0	255, 0, 255	120°, 100%, 100%
azurová (cyan)	0, 255, 255	255, 0, 0	180°, 100%, 100%
modrá	0, 0, 255	255, 255, 0	240°, 100%, 100%
purpurová (magenta)	255, 0, 255	0, 255, 0	300°, 100%, 100%
černá	0, 0, 0	255, 255, 255	0°, 0%, 0%
odstín y šedě	63, 63, 63	191, 191, 191	0°, 0%, 25%
	127, 127, 127	127, 127, 127	0°, 0%, 50%
	191, 191, 191	63, 63, 63	0°, 0%, 75%
bílá	255, 255, 255	0, 0, 0	0°, 0%, 100%
trůvová světlá	255, 192, 192	0, 64, 64	0°, 25%, 100%
trůvová tmavá	255, 128, 128	0, 128, 128	0°, 50%, 100%
tmavá červená	203, 0, 0	52, 255, 255	0°, 100%, 80%
hnědá	128, 0, 0	127, 255, 255	0°, 100%, 50%

Hustota obrazu

Je dána počtem pixelů na jednotku délky,
jednotka: dpi (dots per inch)

- běžná zařízení: monitor cca 100 dpi, tiskárny 300, 600, 1200 dpi, osvitová jednotka až 5000 dpi
- skládání pixelů na výstupním zařízení – snížení hustoty, efektivní hustota

Velikost rastrového obrazu

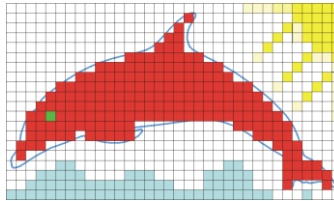
- $V = p \cdot h$
p ... počet pixelů, h ... barevná hloubka v bitech. Výsledek je v bitech.
- Převod na bajty: dělení 8
- Vyjádření počtu pixelů z rozměrů a hustoty obrazu:
 $p = x \cdot y \cdot dx \cdot dy$
x, y ... rozměry; dx, dy ... hustoty
- Obvykle $dx = dy = d$, pak
 $V = x \cdot y \cdot d^2 \cdot h / 8$ [B]

Formáty uložení grafických dat



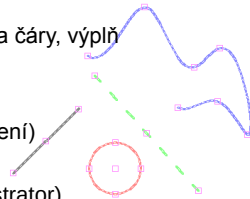
Rastrové (bitmapové) formáty

- obraz je matice pixelů
- pixel má jediný atribut – barvu
- zahrnují většinou komprimaci
- formáty podle počtu barev
 - monochromatické
 - ve stupních šedi
 - barevné
- příklady: BMP, GIF, PCX, TIFF, JPG, PNG



Vektorové formáty

- popis obrazu je posloupnost zakódovaných kreslících příkazů
- jednotlivé formáty slouží různým účelům a výrazně se liší
- prvky vektorových obrazů
 - např. úsečka, oblouk, kružnice, křivka, písmeno
- mají atributy jako
 - pozice, rozměry, barva, tloušťka čáry, výplň
- příklady:
 - DWG (AutoCAD)
 - HPGL (PLT) (pro výstupní zařízení)
 - CDR (CorelDraw)
 - AI, PostScript, PDF (Adobe Illustrator)

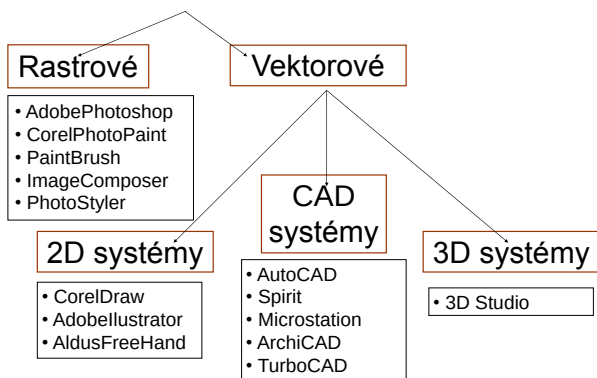


Srovnání formátů

rastrové	vektorové
• pro předlohy z reálného světa • snadné vytváření z dat uložených v poli v paměti • pixelové hodnoty mohou být měněny hromadně • snadný přenos na rastrová výstupní zařízení	• vektorový popis lze snadno editovat • paměťové nároky odpovídají složitosti obrázku • při zobrazování se využívá rozlišení daného zařízení
■ velmi rozsáhlé, zejména pro velké množství barev ■ problémy se změnou velikosti	■ omezená oblast použití ■ někdy horší přenositelnost



Grafické editory



Rastrové editory kreslení a úpravy

- základní geometrické tvary
- typy čar (pero, štětec, ...)
- rozsáhlé možnosti výplní (přechody barev, vzorky, ...)
- guma

GRAFIKA

GRAFIKA



Rastrové editory kreslení a úpravy

- úpravy rastru (barev, velikosti)
- výřezy (kopírování, otočení, posun, zrcadlení)
- retušovací nástroje (zaostření, rozmazání...)
- export do rastrových formátů



Vektorové editory kreslení a úpravy

Vkládání objektů a úpravy jejich vlastností

- základní geometrické objekty
- křivky, kreslení od ruky
- úprava nakreslených objektů (např. kopie, změna velikosti, otáčení, změny pořadí, vzájemné zarovnávání)
- zarovnání vůči sobě, změny pořadí, seskupování
- typ, vzhled a vlastnosti čar a výplní
- široké možnosti práce s textem
- efekty: perspektiva, obálka, tvarové přechody
- export do různých formátů (vektorových i rastrových)

2.2 Datové formáty

Data v počítači

- **Data — formálně vyjádřená skutečnost (symbolicky vyjádřené údaje a hodnoty).**
- v počítači — vše vyjádřeno dvojkovými hodnotami (důvod: technologie výroby počítačů)
- stanovení kódu — nekonečně mnoho možností
- údaje mají množinu povolených hodnot a operací — **datový typ**

Výběr možností uložení

- ze všech teoretických možností lze vybrat způsoby s vhodnými vlastnostmi
- uložení čísel — dvojková soustava se zarovnáním na rozměr paměťových míst, přirozená, celá, racionální čísla
- uložení textu — posloupnost znaků kódovaných podle znakového kódu, ASCII, národní znaky
- ostatní datové typy — většinou lze reprezentovat čísla nebo znaky nebo kombinací

Formát dat (datový formát)

- V operační paměti jsou obvykle data ve tvaru vhodném pro zpracování (výpočty, řazení...)
- Viditelný tvar (tiskárna, displej, klávesnice...) musí být složen výhradně z čitelných (zobrazitelných) znaků

• **Formát dat (datový formát) = způsob (tvar) uložení dat v jakékoliv paměti počítače.**

Souborový formát

- Pojem odvozený z pojmu „datový formát“
- definuje **způsob uložení dat v souboru**.
- Místo popisu dat se používají jména formátů:
PDF, JPG, TXT, PNG, HTML, DOC, XLS, CSV...
- Formáty lze rozdělit na **textové** a **binární**.

5

Textové formáty

- Obsahuje textová data — jen zobrazitelné znaky, konce řádků a případný konec souboru.
- V různých operačních systémech jsou řídící znaky různé:

Operační systém	Konec řádku	Název znaku	Konec souboru	Název znaku
Unix	0a	lf	04	eot
Mac	0d	cr	04	eot
MS	0d 0a	cr lf	1a	esc

6

Textové formáty

- Kódování zobrazitelných znaků je různé.
- ASCII (pozice 0–127) — jednotné
- Textový soubor jen s ASCII: **plain text**
- Národní znaky, speciální znaky — rozdílné
- Textový soubor s národ. znaky: **extended text**

7

Kódování národních znaků

- Znakový kód na 1 B, starší. Příklady:

Kameničtí, PC Latin 2, ISO 8859, Win CP 1250, KOI8čs (ukázky, rozdíl ISO a 1250).

- Znakový kód na větším prostoru: ISO 10646
4 B — velmi neúsporné, stručnější kódování:
2 B Unicode, 1—2 B UTF-8, 2 B UTF 16

8

Významné textové formáty

- CSV — Comma Separated Values (Excel...)
- Zdrojové texty programů
- Řada datových formátů: RTF, PS, SVG, XML

9

Dokument

- Soubor obsahující
 - vlastní text,
 - formátovací značky.
- Podle tvaru značek: textový/binární soubor
- textový: HTML, XML, PostScript, TeX, RTF...
- binární: DOC, SAM, INDD, Text602...

1
0

Binární formáty

- Alespoň část informací vyjádřena jinak než čitelnou posloupností zobrazitelných znaků.
- Výhodné pro okamžité zpracování (formát dat shodný s tvarem v operační paměti)
- Někdy velmi náchylné k chybám, v případě poškození prakticky neopravitelné.
- Možnost utajení formátu, nutnost použití určitého programu, viry...

11

Otevřené a uzavřené formáty

- Souborový formát, jehož specifikace je volně dostupná, je **otevřený**. Formáty **uzavřené** jsou utajovány.
- Uzavřenost formátu umožňuje získat monopol pro jeho zpracování a zároveň silně omezuje možnosti využití uložených dat (CDR, INDD ap., dříve též DOC, XLS, PPT).
- Otevřené formáty jsou prostředkem pro výměnu informací, efektivní využití a zpracování dat (JPG, PDF, PNG, text...).

12

Přenositelnost formátu

- Lze ji pracovně definovat jako **množství programů** schopných zpracovat tento formát.
- Důležitý faktor — zpracování v různých OS.
- Přenositelnost je úzce svázána s otevřeností formátu, ale závisí také na majiteli formátu (srov. DOC, PDF).
- Přenositelnost textových formátů je obecně daleko větší. Binární otevřené formáty rovněž přenositelné.

1
3

Rozpoznání formátu

- **První krok** — rozřídění na textový/binární.
- Využití běžných programů (poznám. blok)
- **Druhý krok** — u rozšířeného textového formátu rozpoznat kódování textu a operační systém, kde soubor vznikl
- U binárních formátů je nutné použít rozpoznávací programy:
- Unix: **file, od**; MS: není nástroj (zkusmo?)

1
4

Asociace formátů a aplikací

- Usnadňuje zpracování dat laikům
- **Princip** — tabulka s řádky: formát -> aplikace (Tento počítač; Nástroje/Možnosti složky)
- **Spouštění aplikace** v případě aktivace souboru příslušného formátu (stažení přes IE, dvojklik v manažeru, výběr v dokumentech...)
- Orientace jen **podle rozšíření (přípony)** jména souboru, může vést ke zmatkům.

1
5

Asociace formátů a aplikací

- **Ideální stav**: 1 formát — 1 aplikace (platí pro speciální případy, např. CDR)
- **Případ 1**: více formátů — 1 aplikace (časté, ale neproblematické)
- **Případ 2**: 1 formát — více aplikací (problém nejednoznačnosti, aktivuje se buď poslední instalovaná aplikace, nebo podle výběru z nabídky. Nepříjemné řešení.)

1
6

Asociace formátů a aplikací

- **Případ 3:** 1 formát — žádná aplikace (chybové hlášení s nabídkou instalovaných aplikací, z nichž uživatel může vybrat — to ovšem prakticky nikdy nevede k úspěchu. XP: rozšíření nabídky programů z Internetu.)
- **Případ 4:** žádný formát — 1 aplikace (buď aplikace žádné formáty nepotřebuje, nebo se jedná o aplikaci DOS nebo o chybnou instalaci.)

1
7

Konverze formátů

- **Změna formátu bez změny informačního obsahu.**
- V praxi — vzácné ideální případy. Často konverze vede ke ztrátě, ale i k nabytí informací.
- **Příklady:** docx -> txt; csv -> xlsx
- Provedení konverze:
 - speciálním programem
 - službami Open a Save (As) běžných programů

1
8

Konverze formátů — příklady

- konverze čísel mezi textovou a binární podobou
- Unix: **convert** — konverze obrazových formátů
- **cstocs** — konverze kódování národních znaků
- Open/Save — úprava dokumentních formátů (např. DOC -> RTF, XLS -> CSV...)

1
9

2.3 Informace v počítači

Jak informaci chápat?

Informace — z hlediska **kvalitativního**

(obsah sdělení, význam zprávy)

tím se zabývá **INFORMATIKA**

Informace — z hlediska **kvantitativního**

(množství a jeho měření)

tím se zabývá **TEORIE INFORMACE**

Údaje, data, informace, znalosti

- Údaj – hodnota libovolné reálné veličiny
- Data – formalizované údaje
- Informace – interpretovaná data
- Znalosti – ucelený komplex informací o nějaké objektivní realitě

Interpretace dat

- Data v počítači: **jedničky a nuly**
- Pro člověka musí být **zobrazeny**
- Zobrazení stejné posloupnosti jedniček a nul může být provedeno **nekonečně mnoha** způsoby
- Interpretace zobrazení: **přisouzení významu** zobrazeným údajům

Pojem datový typ

- Definován oborem **povolených hodnot** a kolekcí **povolených operací**
- **Implementace** – přisouzení posloupnosti binárních hodnot v paměti počítače
- Modeluje objektivní realitu – hodnoty jsou **zobrazeny** pro vstup i výstup
- Příklad: Excel – `formaty.xls`
- Otázka: stejný údaj, kolik nese informace??

Pojem informace

- Mnoho různých definic podle toho, co autoři definice považovali za nejdůležitější.
- **Příklady:**

Různé definice informace

1. Informace je obsah jakéhokoli oznámení, údaje o čemkoli, s určením pro přenos v prostoru a čase. V nejširším slova smyslu je to obsah vztahů mezi materiálními objekty, projevující se změnami těchto objektů.
2. Informace je obsah zprávy, sdělení, objasnění, vysvětlení, poučení.
3. Informace jsou údaje, čísla, znaky, povely, instrukce, příkazy, zprávy apod. Za informace považujeme také podněty a vjemy přijímané a vysílané živými organismy.

Jak informaci měřit?

.**Claude Shannon** — základy **teorie informace**, stanovil možnosti měření informačního množství

.**Shannonova definice informace:**

Informace je míra množství neurčitosti nebo nejistoty o nějakém náhodném ději odstraněná realizací tohoto děje.

.**Informace** rozšiřuje okruh znalostí příjemce.

Měření informačního množství

.**Entropie** — název vypůjčený z termodynamiky, použitý pro měření informačního množství.

.**Jak kvantifikovat rozšíření okruhu znalostí příjemce?**

.**Pravděpodobnost zprávy** — spojeno s individuálními vlastnostmi příjemce (Shannon)

Jevy a jejich realizace

.**Jev** — náhodný proces s n možnými realizacemi
(tah sportky, účast na přednášce, semafor na křižovatce apod.)

.**Realizace jevu** — jeden projev, získání výsledku
(vytažení 6 čísel, konkrétní počet osob na přednášce, svítící zelená na křižovatce apod.)

Požadované vlastnosti funkce pro výpočet množství informace

- Jev X má n realizací, množství informace je funkcí n
- Je-li $n = 1$, jedná se o jev jistý, množství informace je rovno nule
- Jevy X a Y probíhající současně a nezávisle, $p(x,y) = p(x) \cdot p(y)$: množství informace je dáno součtem množství jednotlivých jevů:
 $f(x,y) = f(x) + f(y)$
- Jev X má n realizací, jev Y má m realizací. Je-li $m > n$, pak chceme i $f(m) > f(n)$

Výpočet vlastní informace

- Funkce, která vyhovuje uvedeným podmínkám, je **logaritmus**.

$$I(x) = \log n$$

- Zde předpokládáme, že pravděpodobnost každé realizace je stejná. Má-li jev n realizací, pak můžeme psát

$$p(x) = 1/n, \text{ odsud pak } n = 1/p(x)$$

Výpočet vlastní informace

. **Vlastní informace výsledku realizace x** — je reálné číslo získané logaritmem pravděpodobnosti:

$$I(x) = -\log p(x)$$

. **Základ logaritmu** — principiálně není podstatný. Ale používají se logaritmy o základu 2. Pak dostáváme výsledek v **bitech**.
. Vlastní informace se nazývá též **částečná informace**.

Entropie

.Jak spočítat informační množství celého jevu? — Pomůžeme si shrnutím všech vlastních informací jednotlivých realizací.

.Předpokládejme, že jev X má n realizací $x_1, x_2, \dots, x_n$ s pravděpodobnostmi $p(x_1), p(x_2), \dots, p(x_n)$

Výpočet entropie jevu

.Entropie $H(X)$ je dána určitou střední hodnotou vlastních informací všech realizací jevů:

$$H(X) = - \sum_{i=1}^n p(x_i) \cdot \log p(x_i)$$

.Entropie zahrnující informační množství celého jevu se nazývá též **úplná informace**.

2.4 Přenos dat, kódování

Signál

- Informace má nehmotnou povahu. Přenos musí být proveden nějakým fyzikálním procesem — **nosičem informace**.
- Fyzikální veličinu, která je nosičem informace, nazýváme **signál**.
- Signál lze matematicky modelovat funkcí prostoru a času:

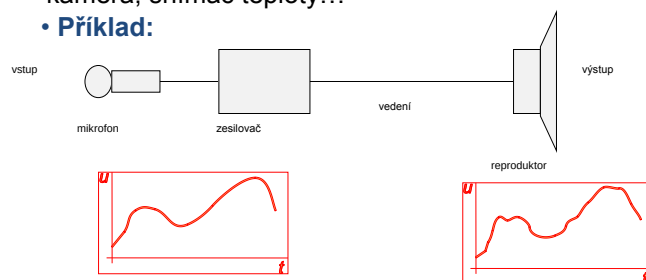
$$s = f(x, y, z, t)$$

Rozdělení signálů

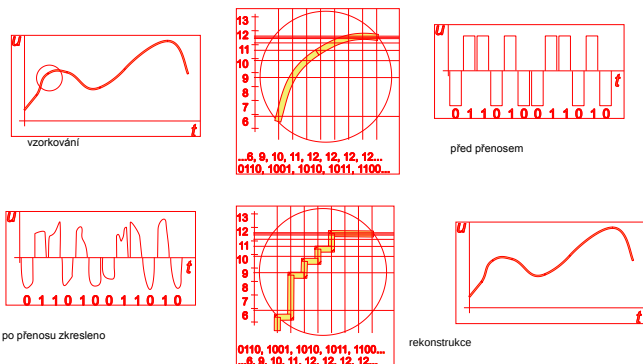
- Všechny signály lze podle časového parametru rozdělit na:
 - **spojité**, každý časový okamžik signálu nese určitou informaci
 - **diskrétní**, signál nese informaci jen v některých okamžicích
 - **statické**, hodnota t nemá vliv na hodnotu signálu
 - **dynamické**, hodnota signálu závisí na hodnotě t

Spojitý signál

- Je vždycky získáván ze vstupu (mikrofon, kamera, snímač teploty...)
- **Příklad:**



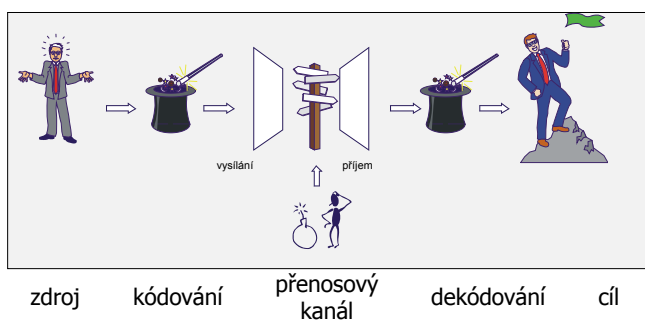
Diskrétní signál



Komunikace

- **Informační vazba** — vzniká mezi dvěma systémy tvorbou, přenosem a výměnou informace
- Informační vazba umožňuje tzv. **komunikaci**.
- Komunikace jedním směrem tvoří **jednoduchý komunikační řetěz**.

Komunikační řetěz



Kódování informace

- Základní podmínkou komunikace je vytvoření **signálního komunikačního kanálu**.
- Informaci je pro tento účel nutné **transformovat**, tj. vyjádřit v jiném jazyce s jinou abecedou.
- Přiřazení znaků jedné abecedy znakům jiné abecedy se nazývá **kódování**, inverzní postup pak **dekódování**.
- Předpis, který toto přiřazování definuje, se nazývá **kód**.

Kvalita kódování, redundance

- Z hlediska optimálního přenosu je efektivní kód, který obsahuje **minimální počet informačních prvků**, každý znak kódu tedy má **maximální entropii**.
- Kvantitativně je hospodárnost kódu vyčíslitelná **redundancí (nadbytečností)**, podle vztahu:

$$R = 1 - H/H_{\max}$$

Způsoby kódování

- **Rovnoměrné Baudotovo kódování** — každému znaku je přiřazen stejně dlouhý kód. Obvykle je jednodušší, rychlejší na zpracování, ale méně hospodárné.
- **Nerovnoměrné kódování** — každému znaku je přiřazen jinak dlouhý kód. Pro konstrukci a zpracování je obtížnější, může však být maximálně hospodárné.

Kódování dat v praxi

- **Kódování elektronické pošty** — způsoby přenosu obecných dat v textové podobě.
- **Přidávání zabezpečovacích informací** — detekce a lokalizace chyb, kontrola úplnosti.
- **Optimalizace uložení** — rychlost ukládání versus velikost uložených dat.

2.5 Zabezpečení informace

Proč zabezpečovat?

- Při přenosu může nastat chyba vlivem **technické nedokonalosti** přenosového kanálu.
- Při přenosu může **nepovolaná osoba číst** přenášená data.
- Při přenosu může **nepovolaná osoba modifikovat** přenášená data.

2

Zabezpečení proti technickým nedokonalostem přenosu

Chyba — změna $0 \rightarrow 1$ nebo $1 \rightarrow 0$

Násobnost chyby — počet chyb v jednotce dat

- jednonásobná chyba (například jedna chyba v přeneseném bytu)
- dvojnásobná chyba, vícenásobná chyba
- četnost chyb s násobností obvykle prudce klesá (například 0,001/s; 0,000 03/s)
- četnost chyb je velmi relativní, záleží na zařízení

Detekce chyby

.Detekce chyby — zjištění, že v přeneseném úseku nastala chyba, není však známo přesné místo.

.Možnosti detekce:

- parita,
- kontrolní součet.

.Obojí na podobném principu.

Detekce chyb s lichou násobností
Jednoduchá realizace
Široké použití

Parita

.**Parita** — doplnění binárních jedniček na:

- sudý počet — **sudá parita**
- lichý počet — **lichá parita**

.**Jednoduchá parita** — jeden paritní bit

.**Kombinovaná parita** — více paritních bitů

Detekce chyby (parita, příklad)

.**Příklad:**

Jednoduchá parita realizovaná devátým bitem

sudá: 01010110 **0**
lichá: 01010110 **1** paritní bit (navíc)

Jednoduchá parita realizovaná osmým bitem (internet)

paritní bit (nejvyšší bit dat) **0**1010110 (sudá)
 11010110 (lichá)

Detekce — kontrolní součty

Kontrolní součet — přídavný údaj vypočtený z dat zvoleným postupem a kontrolovaný stejným postupem na přijímací straně.

Používají se různé varianty pro různé účely:

- podélná parita
- CRC (Cyclic Redundancy Check)
- hashování (otisk prstu, miniatura)
- MD5 (Message-Digest algorithm)
- SHA (Secure Hash Algorithm)

Podélná parita

- Blok dat – operace aritmetického součtu bez přenosu do vyššího řádu

01101010

11001011

00101010

10001011

Každý bit kontrolního součtu doplňuje počet binárních jedniček v příslušném řádu na sudý počet. Proto se kontrolnímu součtu někdy říká **podélná parita**.

Oprava chyb

• **Detekce místa chyby** — pak stačí provést opravu inverzí příslušného bitu.

• **Jednoduchá detekce** — kombinovanou paritou nebo kombinací příčné a podélné parity.

• **Složitější detekce** — použitím samoopravného kódu.

Kombinace parit

• **Chyba se projeví v několika místech** — podle hodnot paritních bitů lze zjistit místo chyby.

01101010

01001011

10101010

10001011

01101010

01011011

10101010

10001011

Samoopravný kód

.Kód schopný detekovat místo chyby. Příklad:
Hammingův kód — založen na existenci povolených a zakázaných kódových kombinací.

.**Hammingova vzdálenost** — určuje se pro dvě hodnoty a je rovna počtu rozdílných bitů.

$x = 011010111010$

$y = 001010101110$

$h = 3$

Princip Hammingova kódu

.**Povolené hodnoty** — kódové kombinace, které mají od sebe navzájem Hammingovu vzdálenost minimálně k .

.**Zakázané hodnoty** — všechny ostatní kódové kombinace. Je jich podstatně více než povolených.

.**Přenos kódové kombinace** — získá-li se po přenosu zakázaná kombinace, buď je detekována chyba, nebo se podle H. vzdálenosti určí nejbližší povolená hodnota.

Detekce a oprava chyby

Kód: 100101101010
(část) 100101101000
100101101001
100101101101
Přenos: 100101100101

povolené hodnoty, $k = 4$

100101100101	→	100101100101	OK
100101100101	→ !	100101101101	Oprava
100101100101	→ !!	100101101001	Detekce

Násobnost chyby $< k/2$... oprava, násobnost $= k/2$... detekce

Zabezpečení proti neoprávněnému čtení

.**Šifrování** — nahrazení (kódování) původních znaků (slov) novými, aby výsledek byl zdánlivě nesmyslný.

.**Steganografie** — věda zabývající se ukrýváním zpráv, nikoliv jejich obsahu.

.**Kryptografie** — věda zabývající se ukrýváním obsahu zpráv tvorbou šifer a jejich aplikací.

.**Kryptoanalýza** — věda zabývající se dešifrováním zpráv bez znalosti klíče (prolamování šifer).

Rozdělení šifer

.**Transpoziční** — znaky mění pořadí, ale zůstávají nezměněny.

.**Substituční** — znaky zůstávají na svých místech, ale mění se (kódují) na jiné.

.**Monoalfabetická** — substituční šifra s jednou tabulkou nahrazení znaků.

.**Polyalfabetická** — substituční šifra s proměnnou tabulkou nahrazení znaků.

Způsoby šifrování

.**Caesarova šifra** — posun znaku v abecedě

PARAPET = OZQZODS

Lze dešifrovat pomocí frekvenční analýzy.

.**Šifra Blaise de Vigenèra (16. stol.)** — posun znaku v abecedě na základě hesla, tj. pro každý výskyt znaku jinak

PARAPET = EEURDTX

Lze dešifrovat pomocí odvození a nalezení hesla.

Vigenèrova šifra

Vigenèrův čtverec:

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
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	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

atd.

Vigenèrova šifra

	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
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	

PARAPET = EEURDTX
PEDROPE

.Šifra rozlomena Charlesem Babbagem v 19. stol.

Enigma

.**Arthur Scherbius (kolem r. 1920)** — první návrhy stroje.

.**Hlavní součástky** — klávesnice, propojovací deska, scramblery, zrcadlo, zobrazení šifry.

.**Princip** — scramblery se otáčejí a mění šifrové písmeno po stisku každé klávesy. Propojovací deska vyměňuje dvojice znaků. Počet kombinací cca 10 na 17.

• Prolomeno v 30. letech (Polsko) a za II. svět. války (Bletchley, Turing), použity tzv. „bomby“

Šifrování v počítačové podobě

- . **Změna frekvenčního spektra** — četnosti kódových znaků nesouvisejí s četnostmi původních znaků.
- . **Šifrovací klíč** — u primitivních způsobů je to kódová tabulka náhrad, u jiných způsobů je to **binární posloupnost** sloužící k šifrování nebo dešifrování.
- . **Symetrický klíč** — pro šifrování i dešifrování je stejný a stejně se aplikuje.
- . **Asymetrický klíč** — klíč má dvě části, pro šifrování a dešifrování slouží různé části klíče.

Symetrické šifrování

- . **Příklad klíče** — 10110 (v praxi bývá například 128 bitů).
- . **Příklad šifrování** — operace XOR (výhradní součet, nonekvivalence).

Data:	10110100 01101011 10110100 00101100
Klíč:	10110101 10101101 01101011 01011010
Šifra:	00000001 11000110 11011111 01110110
Klíč:	10110101 10101101 01101011 01011010
Data:	10110100 01101011 10110100 00101100

Nesymetrické šifrování

- . **Klíč má dvě části** — veřejnou a soukromou (zkráceně veřejný klíč, soukromý klíč).
- . **Použití 1** — pro šifrování veřejný klíč příjemce, pro dešifrování soukromý klíč příjemce:
Zprávu přečte JEN oprávněný příjemce
- . **Použití 2** — pro šifrování soukromý klíč odesílatele, pro dešifrování veřejný klíč odesílatele:
Příjemce dokazuje identitu odesílatele

Distribuce klíčů

.**Certifikační autorita** — „notář“, který osvědčuje, že určitý soukromý klíč vlastní určitá osoba.

Umožňuje dokázat totožnost odesílatele

.**Hlavní funkce CA:**

- generování klíčů;
- přidělování, evidence, obnovování klíčů;
- osvědčování vlastnictví určitého klíče.

Vlastnosti šifrovacích způsobů

.**Symetrické šifrování:**

- jednoduché vytvoření libovolného klíče;
- rychlé;
- libovolná hodnota a délka klíče, neprolomitelné;
- problém s předáním klíče příjemci.

.**Asymetrické šifrování:**

- složitější vytvoření páru klíčů;
- pomalejší;
- délka klíče je známa, méně odolné vůči hrubé síle;
- umožňuje identifikovat odesílatele.

Hybridní šifrování

.**Používá obou druhů klíčů zároveň** — kombinace výhod a zvýšení bezpečnosti přenosu

.**Kombinace klíčů umožňuje aplikovat více funkcí** — zabezpečení proti neoprávněnému čtení, identifikace odesílatele, zabezpečení proti neoprávněné modifikaci.

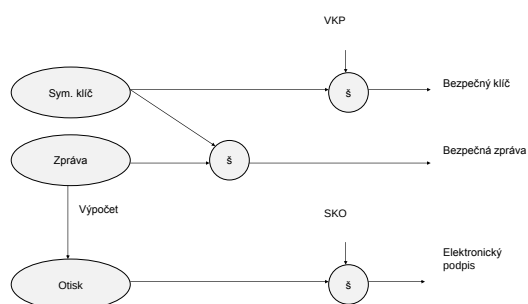
Zabezpečení proti neoprávněné modifikaci

. **Otisk zprávy** — binární posloupnost získaná speciálním algoritmem; je pro každou zprávu jedinečná.

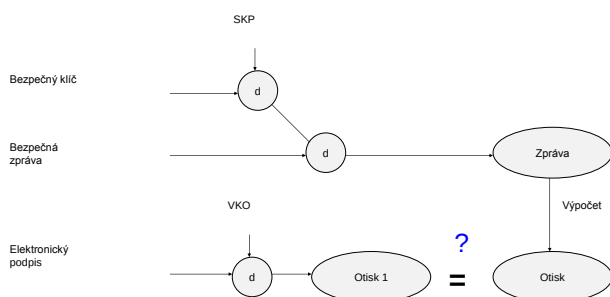
. **Kontrola otisku** — po přenosu zprávy s otiskem se vypočte nový otisk a srovná se s přeneseným.

. **Elektronický podpis** — otisk zašifrovaný soukromým klíčem odesílatele.

Odeslání bezpečné a podepsané zprávy



Přijetí bezpečné a podepsané zprávy



2.6 Komprimace a archivace dat

Potřeba komprimace

- **Redundance v datech** — nutná pro zpracování dat
- **Redundance vzniká:**
 - nedokonalým kódováním dat
 - nutností rychlého přístupu k datům
 - přidáváním zabezpečovacích informací
- **Odstranění (snížení) redundance** — použitím komprimace

2/19

Základní pojmy I

- **Hrubá data** — data před komprimací
- **Komprimovaná (čistá) data** — data po komprimaci
- **Komprimační poměr** — poměr délek hrubých a komprimovaných dat. Vyjadřuje se různým způsobem:
 - h/k — udává násobek hrubých dat
 - $k/h \cdot 100$ — udává, **na kolik** procent se data zmenšují
 - $(1 - k/h) \cdot 100$ — udává, **o kolik** procent se data zmenšují

3/19

Základní pojmy II

- **Záporná komprimace** — data se komprimací zvětšují (nežádoucí jev)
- **Ztrátová komprimace** — některá data se při komprimaci vynechávají
- **Adaptivní komprimace** — komprimační metoda pracuje v závislosti na hrubých datech
- **Symetrická komprimace** — čas komprimace a dekomprimace je stejný

4/19

Komprimační metody

- **Logická komprimace** — jiný (kratší) způsob vyjádření stejných informací; je nutné znát sémantiku dat

Příklady:

- zkracování slov (jako v těsnopise)
- čb fotografie vyjádřená pouze odstíny šedi

- **Fyzická komprimace** — hledání lepšího (kratšího) kódu; nezávisí na sémantice dat

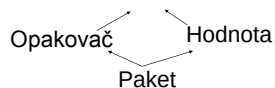
5/19

Metoda RLE

- **Běh** — posloupnost stejných hodnot
- **Run Length Encoding** — kódování délkou běhu
- **Základní princip:**

Hrubá data: 65 65 65 65 78 78 78 32 32 32 32 32

Výsledek: 4 65 3 78 5 32



- **Problém** — střídavá data; může dojít k záporné kompresi. Řeší se speciálním tvarem opakovače.
- Obrazy: **Bitová / bytová / pixelová úroveň**

6/19

Metoda LZW

- **Lempel, Ziv, Welch (1977, vylepšeno 1984)** — algoritmus a jeho implementace
- **Princip:** hledání opakujících se posloupností v hrubých datech a nahrazování jejich výskytů kratším kódem.
- **Postup** — data se analyzují, zjišťují se posloupnosti a jejich opakování. Je-li opakující se posloupnost již ve slovníku, vypisuje se jen její kód.
- **LZMA** — Lempel, Ziv, Markov-Chain Alg., pomalejší, ale lepší komprimační poměr

7/19

Metoda CCITT

- **Princip hledání optimálního kódu** — používá se však pevný slovník
- Implementace: CCITT Group 4 pro monochromatická obrazová data (formát BMP, TIFF, PCX)
- **Vlastnosti:**
 - jednoduchá,
 - závislá na prvcích odpovídajících slovníku,
 - nízký komprimační poměr.

8/19

Vlastnosti uvedených komprimačních metod

- **Metoda RLE:**
 - jednoduchá,
 - závislá na bězích v hrubých datech,
 - nízký komprimační poměr.Použití pro obrazová data, kde se vyskytují běhy.
- **Metoda LZW:**
 - nejsložitější,
 - adaptivní, nezávislá na datech,
 - vysoký komprimační poměr.Univerzální použití. Kvalitu lze ovlivnit hloubkou analýzy dat.

9/19

Implementace

- **Komprimátory** — programy schopné komprimovat, ale také archivovat, pracovat se soubory a adresáři, kryptovat obsah, vkládat poznámky apod.
- **Unix** — gzip, zip
- **OS na PC** — pkzip/pkunzip, arj, WinRAR, WinZip, 7zip atd.
- **Různé komprimátory** — různé formáty archivů, různé ovládání, ale prakticky vždy LZW (LZMA) s mírnými modifikacemi.

10/19

Archivy

- Soubor vytvořený komprimátorem, obsahuje čistá data a režijní informace
- Procento režijní informace závisí na velikosti a počtu komprimovaných souborů
- Formát archivu je pro každý komprimátor jiný
- Moderní komprimátory jsou schopny číst a někdy i vytvářet archivy různých typů

11/19

Vnitřní fragmentace

- Každý disk je složen z alokačních bloků určité délky. Uložený soubor zabírá vždy určitý celočíselný počet alokačních bloků
- Poslední alokační blok souboru není zcela využit – **vnitřní fragmentace**.
- Velikost souboru $\leq$ Velikost na disku
- Shrnutí více souborů do jednoho archivu znamená eliminaci vnitřní fragmentace (i bez komprimace jde o zmenšení prostoru na disku)

12/19

On-line komprimace

- **Implementace uvnitř jiného programu** — služby Otevřít (Open) a Uložit (Save, Save As)
- Při běžné práci se skrytě komprimuje/dekomprimuje.
- Používáno u programů pracujících s vnitřně komprimovanými daty, například obrazové editory, zpracování hudebních dat a videodat.
- Použita symetrická komprimace — čas uložení a otevření je podobný, menší nároky na kvalitu komprimace, často i ztrátová komprimace

13/19

Archivace a zálohování

- **Archivace:**

- uchování dat pro budoucí použití,
- nutnost uchování dokladů o provedených pracích.

- **Zálohování:**

- ochrana před poškozením nebo ztrátou (viry a napadení, požár, povodeň, chyby uživatelů)

- **Vzdálenost kopie:**

- příruční; na stejném disku
 - odkládací; na stejném počítači, ale jiném disku,
 - bezpečnostní; mimo počítač (archivní média).
- Podle vzdálenosti roste i bezpečnost uchování.

14/19

Způsoby zálohování

- Záloha dat, záloha programů
- Zálohují se soubory, adresářové podstromy, disky, systémové soubory a oblasti
- Výchozí záloha
- Úplná záloha
- Rozdílová (diferenciální) záloha
- Přírůstková (inkrementální) záloha
- **PLÁN ZÁLOH**

15/19

Metody a postupy archivace

- **Vytváření archivních souborů** — většinou vhodným komprimátorem nebo specializovanými programy

- **Unix** — program tar (tape archive)

- **OS na PC** — komprimátory, uživatelské dávky

- **Četnost archivace** — podle vzdálenosti archivu: po každé modifikaci dat, jednou denně, jednou týdně, jednou měsíčně...

16/19

Média pro zálohy a archivy

- **Disky** – v počítači (oblast téhož disku, jiný disk, mirror) – zálohy
- **Přenosná média** (optické disky CD, DVD, magnetické pásky, flash disky) – zálohy i archivy (pozor na trvalost záznamu!!)
- **NAS** (Network Attached Storage) – síťově dostupné úložiště – zálohování

17/19

Archivace v prostředí Unix

- **Program tar** a jeho kombinace s bezeztrátovou komprimací gzip; soubory .tar, .tgz
- Vytvoření **skriptu** pro archivaci vybraných souborů a adresářů
- Nastavení času a periodicity archivace – **cron**
- Automatizované **posílání archivů** případně na jiný stroj (připojení disku jiného stroje do souborového systému)

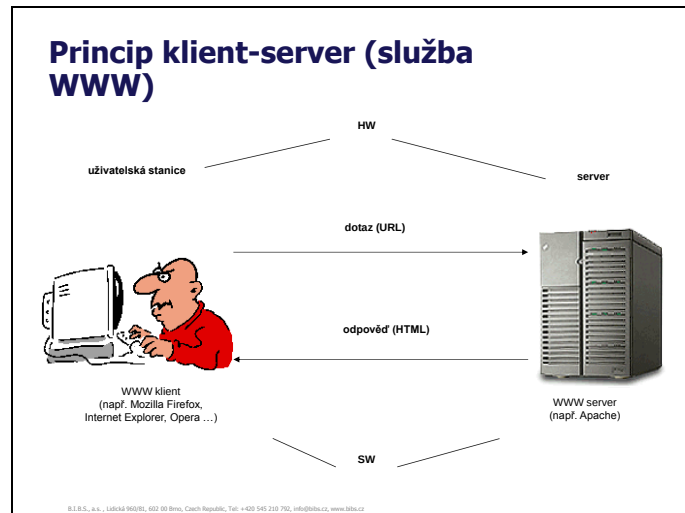
18/19

Archivace ve Windows

- Program **backup**, varianta v příkazovém řádku, nebo interaktivní (i s průvodcem)
- Možnost zálohy **systémových záznamů** a jejich obnova v případě havárie
- **Zálohování souborů** – výběr zdrojů a výběr umístění archivů
- **Plánovač úloh** – možnost volby času zálohování a periodicity

19/19

2.7 Internetové technologie



Princip klient-server

- **Klient** – zahajuje komunikaci, požaduje spojení
- **Server** – poskytuje odezvu klientovi
- **Démon** – program, který neustále běží na serveru a očekává výzvy, při zachycení spustí obsluhu
- **Protokol** – scénář komunikace mezi klientem a serverem, stanovuje pořadí předávání otázek a odpovědí, realizace prostřednictvím portu
- **Port** – identifikace služby ve formě čísla, které klient posílá serveru při zahájení komunikace

8.1.8.5. s.r.o., Lázeňská 96/97II, 602 00 Brno, Czech Republic, Tel: +420 545 210 700, info@8185.cz, www.8185.cz

Nejznámější porty

- **20, 21** – přenos souborů protokolem FTP
- **23** – vzdálený přístup (nešifrovaný, TELNET)
- **22** – vzdálený přístup (šifrovaný, SSH)
- **25** – elektronická pošta (SMTP)
- **80** – služba WWW (HTTP)
- **110** – vzdálený přístup do schránky (POP3)

8.1.8.5. s.r.o., Lázeňská 96/97II, 602 00 Brno, Czech Republic, Tel: +420 545 210 700, info@8185.cz, www.8185.cz

Protokol HTTP

- **HyperText Transfer Protocol**
- Slouží pro přenos objektů libovolného typu (stránky, obrázky, ...) mezi webovým serverem a prohlížečem (klientem)
- Jednoduchý síťový protokol aplikační vrstvy, vlastní přenos dat zajišťuje protokol TCP
- Základní model: navázání spojení → zaslání požadavku klientem → zaslání odpovědi serverem → uzavření spojení

© I.B.S., s.r.o. – učební materiál, 602 00 Brno, Czech Republic, Tel: +420 545 233 750, info@ibscs.cz, www.ibscs.cz

Protokol HTTPS

- Zajišťuje šifrovanou komunikaci mezi klientem a serverem
- Slouží k přenosu informací, které nesmí být nikým odposlechnuty (číslo kreditní karty, heslo)
- Pro šifrování se používá kombinace asymetrické a symetrické šifry se 128bitovým klíčem
- **SSL** (Secure Socket Layer) – norma pro šifrovaný přenos vytvořená společností Netscape

© I.B.S., s.r.o. – učební materiál, 602 00 Brno, Czech Republic, Tel: +420 545 233 750, info@ibscs.cz, www.ibscs.cz

Návratové kódy

- **1xx** – informační, požadavek byl obdržén
- **2xx** – úspěch, dotaz byl pochopen a akceptován
- **3xx** – přesměrování, klient musí provést další akce, aby získal požadovaný dokument
- **4xx** – chyba klienta, byl položen chybný dotaz nebo klient nemá oprávnění získat dokument požadovaný v dotazu (např. 401 = Unauthorized, 403 = Forbidden, 404 = Not Found)
- **5xx** – chyba na straně serveru, není schopen obsloužit požadavek (500 = Internal Server Error)

© I.B.S., s.r.o. – učební materiál, 602 00 Brno, Czech Republic, Tel: +420 545 233 750, info@ibscs.cz, www.ibscs.cz

Omezení HTTP

- Protokol je **bezstavový**
- Server nemá stálé spojení s klienty a nemůže je proto jednoznačně identifikovat
- Velké komplikace pro webové aplikace, které vyžadují stavovou informaci – např. nákupní košík
- Řešení je několik (různé možnosti): detekce IP, cookies, přenášení údajů v URL a skrytých polích formuláře

© J. B. S., s.r.o. – Učební materiál, 602 00 Brno, Czech Republic, Tel: +420 545 233 750, info@jakpsatweb.cz, www.jakpsatweb.cz

Dynamický statický dokument

- **Statický dokument** – vzhled je neměnný, uživatel si nemůže volit zobrazované informace
- **Dynamický dokument** – tvar a prezentované informace může uživatel ovlivnit svojí činností
- **Dynamický dokument na straně klienta** – vytvoření a modifikaci zajišťuje prohlížeč (klient)
- **Dynamický dokument na straně serveru** – vytvořen programem, který běží na vzdáleném stroji (různé technologie – vsuvky, PHP, CGI...)
- **Generovaný dokument** – vytvořen počítačem

© J. B. S., s.r.o. – Učební materiál, 602 00 Brno, Czech Republic, Tel: +420 545 233 750, info@jakpsatweb.cz, www.jakpsatweb.cz

Statické dokumenty WWW

- Textový soubor obsahující značky v jazyce HTML
- Značky v jazyce HTML
 - a) slovní (párové nebo nepárové), mohou mít parametry
 - b) entity
- Vizuální podoba dokumentu – formátování pomocí kaskádových stylů (CSS)
- Způsob zápisu dokumentů v jazyce HTML je popsán ve velkém množství výukových materiálů (např. www.jakpsatweb.cz a mnoho dalších)

© J. B. S., s.r.o. – Učební materiál, 602 00 Brno, Czech Republic, Tel: +420 545 233 750, info@jakpsatweb.cz, www.jakpsatweb.cz

Vlastnosti dynamických dokumentů na straně serveru

- Schopnost řešení složitých a rozsáhlých úloh, používání souborového systému a výkonu serveru
- Nízká závislost na klientovi (prohlížeči) a jeho schopnostech, klient pouze stránku zobrazuje
- Veškeré požadavky a data se včetně odpovědi přenášejí přes síťové spojení (protokol TCP)
- Nelze reagovat na události vzniklé u klienta (pohyb myši, stisk klávesy apod.) – to řeší dynamické dokumenty na straně klienta

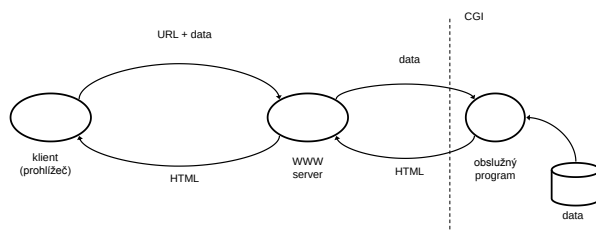
B.Š.Š., s.r.o. – učební materiály, 602 00 Brno, Czech Republic, Tel: +420 545 233 750, info@bsos.cz, www.bsos.cz

Řešení dynamických dokumentů

- **Technologie PHP** – (Pretty Human Pages, Rasmus Lerdorf), jazyk integrovaný do HTML
...<h1>Nadpis</h1>
<? příkazy PHP... ?>...
- **Modul serveru** – například PHP, Perl. Rychlejší odezva
- **Obslužný program na rozhraní CGI** – možnost práce v libovolném jazyce, obecné, avšak někdy časově a výpočetně náročné

B.Š.Š., s.r.o. – učební materiály, 602 00 Brno, Czech Republic, Tel: +420 545 233 750, info@bsos.cz, www.bsos.cz

Obslužný program na rozhraní CGI – základní princip



- **CGI rozhraní** (Common Gateway Interface) – definice způsobu komunikace WWW serveru s obslužnou aplikací (programem)

B.Š.Š., s.r.o. – učební materiály, 602 00 Brno, Czech Republic, Tel: +420 545 233 750, info@bsos.cz, www.bsos.cz

Zpracování požadavku

- URL dynamického dokumentu na straně serveru se liší v datech, zapsaných za otazníkem
`http://akela.mendelu.cz/~xyz/skript.cgi?data`
- Server podle rozšíření `.cgi` pozná, že se jedná o rozhraní CGI, a předá mu data z URL
- Obslužný program zpracuje data a na výstup pošle výsledný text (vygenerovaný dokument)
- Server WWW zašle vytvořený dokument klientovi, který ho zobrazí stejným způsobem jako statické dokumenty

8.1.8.2, s.r.o. - učební materiály, 602 00 Brno, Czech Republic, Tel: +420 545 210 750, info@8182.cz, www.8182.cz

Tvar dat předávaných v URL

- Metoda předání dat (viz formuláře HTML)
 1. **GET** – data předána viditelně v URL
 2. **POST** – data předána skrytě v těle požadavku

```
<form action=skript.cgi method=get>
<input type=text name=prvni>.<br>
<input type=text name=druhy>.<br>
<input type=submit value=odeslat>
</form>
```

```
...skript.cgi?prvni=neco&druhy=neco
```

8.1.8.2, s.r.o. - učební materiály, 602 00 Brno, Czech Republic, Tel: +420 545 210 750, info@8182.cz, www.8182.cz

Kódování URL

- Mezera se v URL zobrazí jako `+` (někdy `%20`)
- Znak, který v URL něco znamená, se kóduje jako `%cc`, kde `cc` jsou dvě šestnáctkové číslice ordinálního čísla znaku. (Unicode `%cc%cc`)
- Příklady

```
value="Jan Kos"
...skript.cgi?jmeno=Jan+Kos

value="Tomáš Hála"
...skript.cgi?jmeno=Tom%E1%9A+H%E1la
```

8.1.8.2, s.r.o. - učební materiály, 602 00 Brno, Czech Republic, Tel: +420 545 210 750, info@8182.cz, www.8182.cz

Proměnné prostředí

- **QUERY_STRING** – obsahuje data předaná v URL
- **REQUEST_METHOD** – metoda předání dat
- **SERVER_NAME** – IP adresa (jméno) serveru
- **SERVER_PROTOCOL** – jméno a verze protokolu
- **SERVER_PORT** – číslo portu hostitele
- **CONTENT_TYPE** – typ dotazovaných dat
- **HTTP_USER_AGENT** – prohlížeč
- **REMOTE_ADDR** – IP adresa klienta
- ...a mnohé další (nejdůležitější jsou první dvě)

B.Č.Č., s.r.o., IČ000 00000, 000 00 0000, Czech Republic, Tel: +420 500 200 700, info@bccc.com, www.bccc.com

Předávání dat na rozhraní CGI

- **Vstup dat do obslužného programu**
 - z proměnné **QUERY_STRING**
v případě, že jsou data předávána metodou GET
 - ze standardního vstupu
v případě, že jsou data předávána metodou POST
- **Výstup dat z obslužného programu**
 - výpis na standardní výstup

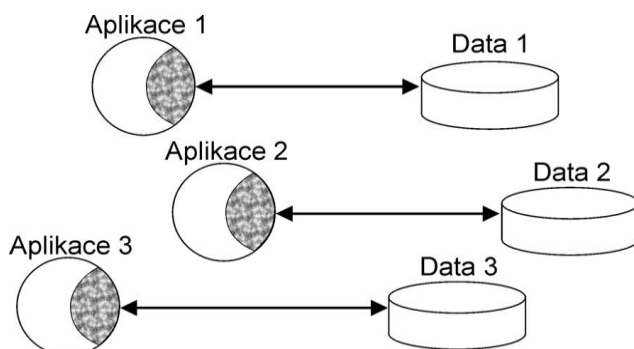
B.Č.Č., s.r.o., IČ000 00000, 000 00 0000, Czech Republic, Tel: +420 500 200 700, info@bccc.com, www.bccc.com

2.8 Databázové systémy

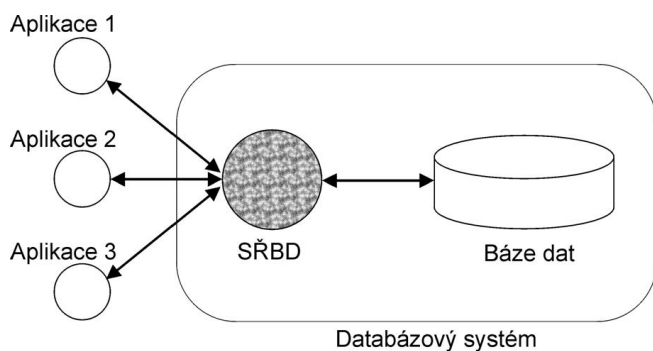
Typy aplikačních programů

- **Programy pro vědeckotechnické výpočty**
 - minimální vstupy a výstupy
 - převládá zpracování údajů v procesoru (mnoho výpočtů podle složitých algoritmů)
- **Programy pro hromadné zpracování dat**
 - převažující operací jsou vstupy a výstupy
 - minimální zpracování údajů (jednoduché operace – průměry, součty, ...)

Agendové zpracování dat



Pojem báze dat, SŘBD



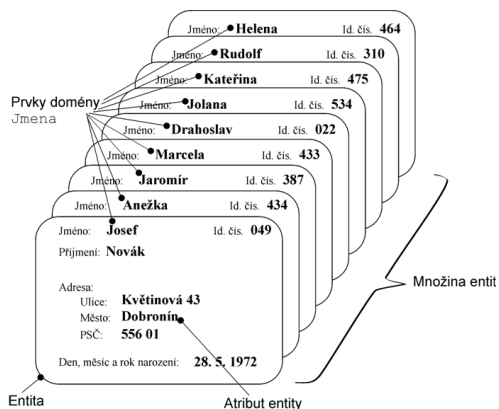
Databázový systém

- Společné označení pro data uchovávaná v centrálně zpracovávané struktuře dat zvané báze dat a pro obslužné speciální programové vybavení nazývané systém řízení báze dat (SŘBD) (Database Management System — DBMS)

Informace v bázi dat

- **Entity**
 - údaje o objektech reálného světa
 - skládají se z jednotlivých položek (například entita Osoba, položky Jméno, Příjmení, Rodné číslo, Adresa)
- **Vztahy**
 - údaje o vazbách mezi entitami
 - v mnoha případech jsou důležitější než samotné entity
- **Integrovní omezení**
 - podmínky kladené na data

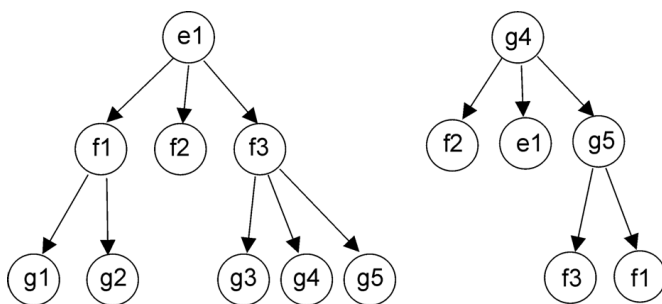
Entity a jejich popis



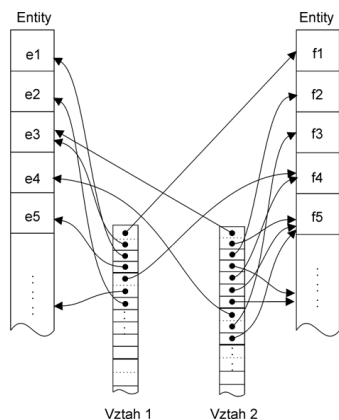
Modelování vztahů mezi entitami

- SŘBD se vzhledem k aplikacím chová určitým způsobem – předstírá určité uložení vztahů
- Vztahy mohou být uloženy explicitním nebo implicitním způsobem
- Typy vztahů: $1 : 1$, $1 : N$, $M : N$
- SŘBD odpovídá jistým modelům – hierarchický, síťový, relační – klasifikovaným podle realizace vztahů mezi entitami v bázi dat

Hierarchický model SŘBD



Síťový model SŘBD



Relační model SŘBD

- SŘBD je postaven na **matematické definici** relace
- Relace je **podmnožinou kartézského součinu** doménových množin, reprezentuje tedy univerzální vyjádření vztahů

$$R \subset D_1 \times D_2 \times \dots \times D_n$$

- Relace mohou být reprezentovány **množinovým zápisem**, **tabulkou** (řádky představují prvky, sloupce pak atributy) nebo souborovým **záznamem** (položky každého záznamu jsou stejně uspořádány)

Operace nad relacemi

- **množinové** – sjednocení, průnik, rozdíl, doplněk
- **databázové** – restrikce, projekce, spojení
implementují se ve všech databázových systémech

Restrikce

- Restrikcí se rozumí **výběr prvků** relace, vyhovujících určité, tzv. **restrikční podmínce** vyhodnocované pro každý prvek zvlášť
- **Příklad:** výběr zaměstnanců z tabulky ZAM, kteří mají plat menší než 20000 Kč

ZAM

rc	jmeno	prijmeni	plat	utvar
7812154138	Petr	Novák	18000	101
6509031234	Jan	Starý	19000	100
6910284321	Daniel	Novotný	22000	101

rc	jmeno	prijmeni	plat	utvar
7812154138	Petr	Novák	18000	101
6509031234	Jan	Starý	19000	100

Projekce

ZAM

rc	jmeno	prijmeni	plat	utvar
7812154138	Petr	Novák	18000	101
6509031234	Jan	Starý	19000	100
6910284321	Daniel	Novotný	22000	101
7305113412	Václav	Novák	18000	100

- Projekcí se rozumí **výběr domén** (atributů)

- **Příklad:** zobrazení jen příjmení a platu zaměstnanců

prijmeni	plat
Novák	18000
Starý	19000
Novotný	22000

- **Příklad:** kombinace restrikce a projekce: zobrazení příjmení a platu zaměstnanců, kteří pracují v útvaru 101

prijmeni	plat
Novák	18000
Novotný	22000

Spojení

- Spojením dvou relací se rozumí relace obsahující **atributy původních relací** s prvky, které splňují **spojovací podmínku** ve společném atributu obou relací

ZAM

rc	jmeno	prijmeni	plat	utvar
7812154138	Petr	Novák	18000	101
6509031234	Jan	Starý	19000	100
6910284321	Daniel	Novotný	22000	101

ODD

utvar	nazev
100	sklad
101	výroba

- **Příklad:** spojení údajů z obou tabulek tak, aby u každého zaměstnance byl i název oddělení (s projekcí do tří atributů)

jmeno	prijmeni	nazev
Petr	Novák	výroba
Jan	Starý	sklad
Daniel	Novotný	výroba

Vazby mezi tabulkami

- Provázání tabulek pomocí identifikátorů
- Identifikátor řádku – číselný, složený (kandidátní klíč)
- Primární klíč – jednoznačně určuje prvek relace
- Cizí klíč – určuje vazbu mezi relacemi pomocí přirozeného spojení
- **E-R diagram** (konceptuální schéma) – grafický návrh tabulek a vazeb mezi nimi

ZAM

rc	jmeno	prijmeni	plat	utvar
7812154138	Petr	Novák	18000	101
6509031234	Jan	Starý	19000	100
6910284321	Daniel	Novotný	22000	101

ODD

utvar	nazev
100	sklad
101	výroba

Normální formy báze dat

- **První normální forma**

- jednotlivé atributy relace musí být atomické

rc	jmeno	prijmeni	plat	děti
7812154138	Petr	Novák	18000	Jana, Pavel

- **Druhá normální forma**

- neklíčové atributy musí záviset na primárním klíči

rc	jmeno	prijmeni	plat	úkol
7812154138	Petr	Novák	18000	413

- **Třetí normální forma**

- neklíčové atributy musí být navzájem nezávislé

rc	jmeno	prijmeni	plat	utvar	nazev
7812154138	Petr	Novák	18000	101	výroba

Implementace databází

- **Stolní systémy**

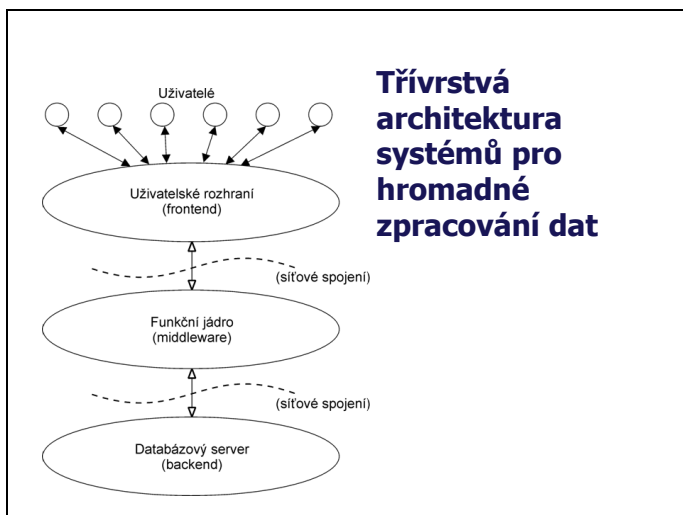
- relativně malé objemy dat
 - jednoduchá obsluha
 - nízká úroveň zabezpečení
 - důraz na interaktivní ovládání

- **Velké systémy**

- relativně velké objemy dat
 - vzdálený přístup k datům
 - obsluha přes unifikované rozhraní, jazyk SQL
 - zabezpečení dat proti ztrátě, proti narušení
 - ovládání prostřednictvím různých klientů

Charakteristické vlastnosti současných SRBD

- Transakční zpracování
- Zotavení chyb
- Souběžný přístup více uživatelů
- Ochrana dat
- Variabilní architektura dat (centralizované nebo distribuované uložení dat)
- Zpracování v reálném čase
- Práce s multimediálními daty



2.9 Informační systémy

Základní pojmy

- **Informace** jsou data, kterým jejich uživatel přisuzuje určitý význam a které uspokojují konkrétní objektivní informační potřebu svého příjemce. Informace tedy vznikají z dat až v okamžiku jejich užití.
(Informace představuje vypovídací schopnost dat, vzniká zpracováním dat a je cílem tohoto zpracování.)
- **Systém**
„Systém je komplex prvků nacházejících se ve vzájemné interakci“ (Bertalanfy).

Základní pojmy (pokr.)

- **Informační systém (IS)** je komplex informací, lidí, informačních technologií, technických prostředků a metod sloužících ke sběru, přenosu, uchování a zpracování dat za účelem tvorby a prezentace informací.
- **IS** je nějakým způsobem organizován a začleněn do organizační struktury podniku, má určité ekonomické charakteristiky a musí být určitým způsobem řízen jak v době jeho budování tak v době jeho fungování.
- **Základním úkolem IS je**
 - Sběr informací.
 - Uchování a zpracování informací do požadovaného tvaru příp. rozsahu.
 - Předání informací řídicím úrovním včas.

Základní pojmy (pokr.)

- Obsah IS můžeme vyměřit těmito hlavními charakteristikami:
 - **Funkcemi**, funkcionalitou IS (hierarchicky uspořádaný souhrn všech operací s daty).
 - **Procesy**, které podporuje. IS by měl v co největší míře podporovat optimalizaci podnikových procesů (procesní řízení firmy).
 - **Daty**, datovými zdroji, které jsou předmětem zpracování v rámci funkcí a procesů IS.

Hospodářské prostředí a IS/IT

- **Nová ekonomika je založená** na znalostech a myšlenkách, kde klíčem k tvorbě nových pracovních příležitostí a ke zvyšování životní úrovně jsou inovátorské nápady a technologie integrovaná ve službách a výrobcích. Je to ekonomika, kde riziko, nejistota a neustálá změna jsou spíše pravidlem, než výjimkou.
- Novou ekonomiku **reprezentují** především tato **odvětví**: informační technologie, internet, telekomunikace, biotechnologie.

Rysy současné společnosti ve vztahu k IS

- Důvěra v SW rychle roste.
- Aplikace jsou rozsáhlejší, komplexnější a náročnější.
- Konkurenční prostředí vyžaduje rychlejší nasazení IS.
- Roste potřeba rychlé, včasné a správné informace.
- Informace souvisí se znalostmi.
- Podniky vydávají nebývalé investiční prostředky na IS.

Uživatel a jeho požadavky

- IS by měl podporovat strategickou orientaci podniku.
- IS by měl mít odpovídající funkční spektrum.
- IS by měl být integrovaný, otevřený a jednoduchý.
- IS by měl být flexibilní a udržitelný.
- IS by měl být efektivně provozuschopný.

Řešitel a uživatel

- Snahou podniků je pracovat s integrovaným plně automatizovaným IS, který slouží vedení podniku na všech úrovních řízení a ve všech oblastech jeho aktivit. Používá se pojem podnikový informační systém.
- Řešitel i uživatel musí kvalitně komunikovat.
- **Řešitel** je často tzv. systémový integrátor (proces outsourcingu).
- **Uživatel** je nejen koncový pracovník, který bude systém využívat a vkládat do něj data, ale také management všech úrovní, který bude systém využívat pro účely rozhodování, případně **zadavatel**, který bude řídit vývoj a financování IS.

ASW (Aplikační software)

- **Aplikační software ASW (aplikační programové vybavení)** – systém, jehož cílem je počítačová podpora částí informačních systémů.
 - **Individuální ASW** – specifické aplikační systémy pro individuálního zákazníka (organizaci) dle jeho požadavků.
 - **Technologicky orientovaný ASW** – OIS, např. MS OFFICE.
 - **Věcně orientovaný ASW** – TASW (typový ASW)
Vlastnosti TASW – modulový princip architektury, vysoká parametrizace, komplexnost a vysoká vnitřní složitost, vnitřní integrace s OIS, integrace datové základny.

ASW (Aplikační software)

Řešení IS v podniku lze realizovat třemi způsoby:

- Vývojem specializovaného „jednoúčelového“ SW.
- Nákupem a instalací TASW.
- Komplexními projekty založenými na výběru velkých aplikačních SW, customizací a dořešením těch modulů, které chybí nebo neodpovídají potřebám zákazníka.

Tvorba IS

- **Tvorba IS** je vývoj programového vybavení včetně hardwarového pozadí, bezpečnostních mechanismů či pracovních postupů a doporučení.
- Tvorbě nového IS nebo inovaci starého IS předchází pečlivý **popis a hodnocení současného stavu a definování cílového stavu**.
- Bere se v úvahu
 - Analýza stavu IS konkurence nebo klíčových partnerů
 - Hodnocení stávajícího aplikačního software
 - Trendy IS
 - Výsledky SWOT analýzy
 - Podnikové cíle, priority podniku
 - Požadavky uživatelů.

Projektování a analýza IS

- Nejprve je nutné systém **zobrazit a popsat**, aby mohl být pochopen.
- Dále je nutné vytvořit **model systému** a ten pak zkoumat.
- Celý projekt tvorby IS je složen z činností a úloh, které tvoří „**životní cyklus vývoje**“ systému, System Development Life Cycle“.
- **Fáze životního cyklu** (studie, analýza, návrh, testování, zavedení, provoz a údržba).

Projektování a analýza IS

- Dva **extrémy** orientace v projektování:
 - **Technokratická** – aplikace je plně podřízena potřebám a schopnostem výpočetní techniky.
 - **Uživatelská** – cílem uživatele je přizpůsobení IS stávající práci, stávajícím formám dokladů a sestav.
- **V praxi** jde o kombinaci obou, dohodou mezi řešiteli a uživateli. Uživatelské potřeby jsou rozděleny do modulů, subsystémů, ty jsou navzájem propojeny.

Přístupy k tvorbě IS

- **Ad hoc**
 - Svoboda tvorby
 - Vlastní zkušenosti
 - Snaha projektantů vyhnout se problémům.
- **Fundamentalistický přístup**
 - Striktní používání daných postupů.
- **Vyvážený přístup**
 - Kombinace systematickosti a kázně s potřebnou tvůrčí volností.

Metody popisu analyzovaného systému

- **Cílem analýzy** je popsat systém:
 - **Neformálně**
 - **Formálně**
 - V dnešní době se prosazují formalizační metody, je nutné zvládnout jazyk používaný pro formalizaci, používají se formalizované modely.
 - Je možné simulovat různé postupy, situace a prověřit správnost analýzy například testováním na vzorku zkušebních dat.
 - Analytici dnes používají metody založené na **systémovém přístupu** (strukturované a objektové metody) případně **metodu prototypování**.

Postup práce analytika

- **Zmapuje** stávající systém (zjistí strukturu, prvky, vazby mezi nimi).
- Vytvoří logické **modely** systému.
- **Komunikuje** nad modely s uživateli a zadavateli.
- Provede důkladnou **dokumentaci** schválených modelů.
- V některých případech vytvoří a představí **prototyp**.

Efektivnost zavádění IS

- **Efektivnost** je účinnost prostředků vložených do nějaké činnosti hodnocená z hlediska užitečného výsledku této činnosti.
- Zatímco **výdaje** do IS jsou viditelné, **přínosy** jsou neviditelné, nelze tedy prokázat konzistentní vztah mezi výdaji na IS a ukazateli úspěšnosti podniku.
- Pro určování efektivnosti se používají **základní** (náklady a výnosy) a **doplňkové ukazatele a rovnice pro dobu návratnosti**.

Náklady a přínosy

- **Náklady**
 - **Jednorázové**
 - Náklady na vývoj IS (dočasné vybavení pracovišť, konzultace, cestovné...)
 - Náklady na investice (HW, SW, realizace sítě...)
 - Náklady na vlastní implementaci IS (konverze dat, školení pracovníků...).
 - **Pravidelné roční**
 - Stálé (odpisy, mzdy, energie, údržba SW, HW...)
 - Variabilní (cestovné, penále, doprava, kurzy...).

Náklady a přínosy

- **Přínosy**
 - **Kvantifikovatelné**
 - Jednorázové (prodej projektu IS)
 - Roční (zvýšení výroby, zvýšení odbytu, snížení nákladů, úspora pracovníků, nižší skladové zásoby...).
 - **Nekvantifikovatelné**
 - Zjednodušení a urychlení přístupu k informacím
 - Kvalitnější evidence
 - Přesnější zpracování informací
 - Zlepšení jména firmy, efektivnější práce, kvalitnější vztah se zákazníkem...
