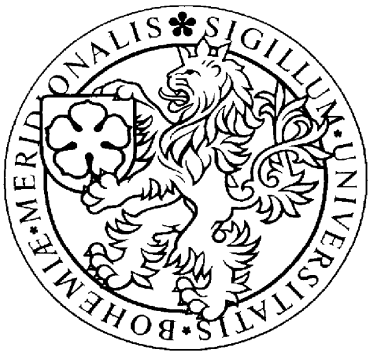
JIHOČESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH
Zdravotně sociální fakulta



KOMUNIKACE A INFORMAČNÍ SYSTÉMY

doplňkové texty pro posluchače kombinované formy studia studijního programu „Ochrana obyvatelstva“

studijního oboru „Civilní nouzová připravenost“

ČESKÉ BUDĚJOVICE 2007

Klíčová slova: bezpečnostní, data, komunikace, média, technologie

ÚVOD

Předložený text je určen jako opora pro orientaci posluchačů studijního programu „Krizové řízení zaměřené pro potřeby zdravotnictví“ v předmětu Komunikace a informační systémy. Je rozdělen do čtrnácti kapitol, z nichž většina z důvodu souvisejících témat je sloučena do dvojbloků a k nim je uvedena doporučená literatura, www stránky k samostudiu a pomocné otázky. I přesto stěžejní část výuky bude provedena na přednáškách z důvodu vysvětlení pojmů a souvislostí ve vztahu ke studovanému oboru.

PŘEHLED KAPITOL:

1. Obecný úvod do problematiky, způsoby komunikace
2. Základní přístupy k informačním tokům
3. Popis jednotlivých komunikačních technologií, lokální a vzdálené přístupy I
4. Popis jednotlivých komunikačních technologií, lokální a vzdálené přístupy II
5. Způsoby ukládání dat, databázové systémy
6. Architektura databázových systémů, architektura Klient – Server
7. Standardy ISVS (Informačního systému veřejné správy)
8. Geografické informační systémy, UIR-ADR (Územně identifikační registr adres)
9. Bezpečnostní zásady při ochraně dat, zásady a konkrétní postupy při bezpečném přístupu k informacím
10. Využití Internetu jako zdroje dat, popis funkcionality, přístupy
11. Veřejně dostupné zdroje informací
12. Zásady tvorby informační podpory, analýza problému, návrh struktury dat I.
13. Zásady tvorby informační podpory, analýza problému, návrh struktury dat II.
14. Legislativa v oblasti přístupu k informacím a ochrany dat

1. a 2.Obecný úvod do problematiky, způsoby komunikace, základní přístupy k informačním tokům

Tento předmět si klade za cíl přístupnou formou vysvětlit využití moderních komunikačních a informačních technologií a prostředků v přístupu k informacím. Přístup k informacím zásadním způsobem ovlivňuje myšlení a práci lidí ve všech sférách a oborech činností. Zvláště umění získat a zpracovat informace pro potřeby operačního a krizového řízené v reálném čase jsou zásadní pro správné rozhodnutí. Pokud nemá člověk obavu z výpočetní techniky, tedy prostředku umožňující přístup k informačních zdrojům získaných na elektronických médiích, Internetu a dalších úložištích, najde nejrychlejší a nejobsáhlejší zdroj přístupu k informacím. A obavu a ostych z nových technologií ztratí tehdy, kdy se s ní naučí rutinně a bez obav pracovat. Výklad látky bude zaměřen na důležité body nebo úseky v oblasti informatiky vycházejí z praktických znalostí a zkušeností v oboru informatiky a operativní činnosti v základní složce IZS.

Generace, která se dostává v této době do produktivního věku, již má jistou tzv. počítačovou gramotnost a lze tedy předpokládat, že není potřeba posluchače seznamovat se základními periferiemi osobních počítačů ani je učit základům psaní na klávesnici a ovládání myši. Stejně tak se již předpokládá základní znalost práce s operačním systémem, textovými a tabulkovými procesory i elektronickou poštou a Internetem. Ale i zde z praktických zkušeností s čerstvými absolventy vysokých škol, které nejsou zaměřeny na informatiku, se setkáváme s problémy, které vyvěrají z ne úplně zvládnuté problematiky základních způsobů ukládání dat, hierarchie stromové struktury adresářů a práce se soubory, s ukládáním dat jak na pevné disky, tak na jiná média. Uživatel osobního počítače je dnes sám sobě správcem dat a správou počítače je vlastně neustálý přesun a manipulace s daty. Právě rutinní zvládnutí těchto operací je základem k bezproblémovému ovládání aplikací, které jsou bránou do informačních systémů.

Výklad k cestě za daty začneme na lokální stanici a lokálních médiích, tedy pevných a flash discích, DAT, CD,DVD s krátkou připomínkou historie (děrné štítky, děrné pásky, magnetické pásy, diskety apod.), výkladem základního popisu práce osobního počítače a způsobu ukládání dat ve smyslu pochopení interakce mezi strojem a uživatelem. Tento výklad bude mít za cíl pochopit, co v určitých časových intervalech počítač dělá nebo má dělat a tento stav nám napoví, zda operace, které na počítači provádíme probíhá správným směrem a minimalizuje čas strávený při práci s výpočetní technikou k získání potřebného výsledku.

V další fázi bude následovat vydání se za daty mimo lokální stanici, tedy popisu práce počítačů v síti, nejprve lokální a dále metropolitní a rozsáhlé a to jak po pevných médiích (metalická a optická vedení), tak bezdrátově. Popis způsobů práce počítačů v síti, jejich technologie přenosů, ale v neposlední řadě i protokolů, se kterými sítě pracují, je důležitý pro pochopení, jaká forma přístupu je vhodná pro získání konkrétních dat v závislosti na jejich formě, obsahu a objemu.

Elektronická data musí být někde uložena a vhodnou formou pro uživatele zobrazena. Způsoby ukládání dat a hlavně systém ukládání dat, tedy databáze, budou náplní dalších přednášek. Zde se posluchač dozví jak historii a současnost, tak nové trendy ve způsobu ukládání dat jak na samotná média, tak ve způsobu organizace ukládání dat, tedy základní uložení v souborech a strukturálně v databázích. Nebude opomenuto ani vyjmenování zásad

pro zabezpečení uložení dat a způsoby zálohování dat. Právě práce s daty uložených v databázích může být pro posluchače v jejich další praxi každodenní práce. Způsoby zobrazení dat budou popsány od základní formy - práce s aplikací až po obecný přístup např. standardizovanými prostředky (jazyk SQL).

V druhé polovině přednášek budou popsána již konkrétní informační systémy, nejprve standardizace ve státní správě a jejich informační systémy, registry, geografické informační systémy a existující informační zdroje a geografická díla. Na tuto tématiku naváže blok přednášek se zaměřením k zabezpečenému přístupu k datů, AAA (Autorizace, Autentizace, Acounting) a základy bezpečností politiky v ochraně dat (zabezpečené protokoly, zabezpečené přístupy). S takovouto průpravou bude možno se pustit do práce s daty v nebezpečných vodách sítě Internet s konkrétní návštěvou veřejně přístupných zdrojů,. Poslední blok bude zaměřen na vysvětlení zásad pro návrh a vlastní tvorbu informačního systému od analýzy problematiky po návrh databázové struktury. Látka bude zakončena náhledem do legislativy v oblasti informatiky.

Způsoby komunikace

Komunikace je hnací silou celého lidstva. Když opomeneme základní komunikační prostředky jako je dotyk, pohled , mimika, gestikulace, zvuky a vývojovým vrcholem řeč, jednalo se vždy o komunikaci na velmi malou vzdálenost, tedy lokální. Touha domluvit se na větší vzdálenosti započala zvukovými kouřovými a světelnými signály, které byly účinné v závislosti na fyzikálních zákonech a klimatických podmínkách. Nejvyšší vývojové stádium představoval optický telegraf bratří Chappéů sestrojený koncem 18.století ve Francii na základě konstrukce se sestavou pák a ramen na kopci, kde předem dohodnutým klíčem pohybů došlo k předání informací a tento systém byl použit v době Napoleonských válek. Až na počátku 19. století byl prvním zásadním impulsem v oblasti komunikace vynález elektrického telegrafu a telegrafní sítě, kterou bylo možno odesílat pouze kódované signály (Morse). Velmi rychle proto následovalo vylepšení, kterým bylo možno po kabelu přenášet lidský hlas a to telefon a budování rozsáhlých telefonních sítí založené na technologii přepínání okruhů, která byla v USA a Evropě v celoplošném měřítku dokončena v druhé polovině 20. století.

Potřeba komunikace se přenesla po vynálezu prvních počítačů logicky i do této oblasti. Technologie přepínání okruhů byla vhodná pro přenos hlasu, kde potřeba přenosu dat je víceméně kontinuální narozdíl od počítačových dat, která mají tendenci být zasílána po skupinkách a úseky extrémní aktivity jsou střídána s úseky aktivity malé. Rozvoji sítí přispěl objev technologie přepínání paketů. Spojení touto technologií není vytvořeno na celou dobu přenosu, ale každý paket si může v rozsáhlé síti zvolit jinou cestu a pak komunikace z mnoha různých zdrojů mohou spolu sdílet jednu společnou trasu. Tím byl dán základ k budování moderních sítí vedoucí do podoby technologií používaných v rozsáhlých datových sítích i celosvětové síti Internet.

Základní přístupy k informačním tokům

Přístupem k informacím může být myšlena cesta za informací, ale i forma přístupu k získání informace. Cesta i forma byla vždy poplatná vývojovému stupni společnosti.

Způsob a cestu přístupu lze rozlišovat například dle následujících kritérií:

Přístup pasivní - získávání informací bez vlastní aktivity (poslouchání zpráv z médií)
Přístup aktivní - získávání informací vlastní vůlí a činností (studium, cílené získávání informací)

Informace lze získávat z jednoho zdroje (bez ověření) nebo z více zdrojů, bez nutnosti pohybu za informací - místně (lokálně) nebo s nutností pohybu za informací - přístup vzdálený , je nutné propojení s okolním světem.
Moderní informační systémy používají podobné principy v přístupu k informacím. Analogicky lze popsat i základní způsoby přístupu k informacím u osobních počítačů a počítačových sítí a tvorba architektury přístupu k datům byla inspirována obecnými pravidly z běžného života. Podle vzdálenosti a typu média, po kterém za informací putujeme nebo informace putuje k nám se ustálila počítačová terminologie na následujících definicích:

Místní přístup -v rámci datových médií uložených v osobním počítači a jeho periferních úložištích

Vzdálený přístup

- mezi počítači v rámci budovy nebo objektu
    - spojení dvou počítačů
    - počítačová síť Ad Hoc
    - lokální počítačová síť LAN (Local Area Network)
- vzdálený přístup mezi počítači v rámci rozlohy odpovídající městské aglomeraci – MAN (Metropolitan Area Network)
- vzdálený přístup mezi počítači na větší vzdálenost, rozsáhlé počítačové sítě - WAN (World Area Network). V dnešní době nejvyužívanější přístup k informacím - Internet patří jednoznačně do této skupiny

Doporučená literatura:

1. Shinder, D.L.: Počítačové sítě. Cisco Press 2001,autor.překlad SoftPress s.r.o. 2003
2. Pužmanová, R.: Širokopásmový Internet. Computer Press Brno 2004

3. a 4. Popis jednotlivých komunikačních technologií, lokální a vzdálené přístupy

K tomu, aby spolu mohly počítače komunikovat, musí být nějakým způsobem propojeny. Historie zaznamenala množství způsobů a technologií propojení, které by vystačily na samostatný předmět. Rozsah potřebný pro Vaše znalosti je možný zúžit na historicky zásadní používaná rozhraní a rozhraní využívaná v současnosti do té míry, aby vám tyto informace byly ku prospěchu jako uživatelům informačních systémů. I přesto se alespoň v základních principech musíme dotknout teorie, kterou zahájíme popisem topologie sítí, typy sítí a funkcionalitu budeme interpretovat na základním modelu ISO OSI:

Topologie sítí:

- Sběrnicová (typický představitel Ethernet 10BASE2 na koax.kabelu)
- Hvězdicová (typický představitel Ethernet 10BASE-T, 100BASE-TX na kroucené dvojlince)
- Kruhová (prstencová - typický představitel Token - Ring)

Typy sítí:

- PAN
- LAN
- MAN
- WAN

PAN - Personal Area Network - personální síť spojující prostředky v rámci prostoru v řádu desítky až několika desítek metrů od uživatele - persony
Typický představitel - Bluetooth (od verze 1.1 dle IEEE 802.15.1)

LAN - Local Area Network - lokální síť spojující počítače v rámci rozlohy budovy, objektu nebo areálu. Historie:

- Ethernet na tenkém koaxiálním kabelu (10BASE2) dle IEEE 802.3
- Ethernet 10BASE-T, 100BASE-TX, 1000BASE-CX, kabel kroucená dvojlinka UTP, STP (Unshield a Shield Twisted Pair) dle IEEE 802.3
- Bezdrátový přenos dle IEEE 802.11

MAN (Metropolitan Area Network) - vzdálený přístup mezi počítači v rámci rozlohy odpovídající městské aglomeraci

WAN (World Area Network) - vzdálený přístup mezi počítači na větší vzdálenost, rozsáhlé počítačové sítě

Vrstvy OSI (Layers)

1. Fyzická vrstva (Physical Layer)
2. Linková (spojová) vrstva (Data Link Layer)
3. Síťová vrstva (Network Layer)
4. Transportní vrstva (Transport Layer)
5. Relační vrstva (Session Layer)
6. Prezentační vrstva (Presentation Layer)
7. Aplikační vrstva (Application Layer)

Fyzická vrstva tedy zabezpečuje komunikaci zařízení na fyzické úrovni, tedy se jedná vlastně o přenos po médiu. To může být metalické, optické nebo používat frekvenci bezdrátového připojení. Popisuje tedy elektrické či optické signály. Na fyzické vrstvě se používají např. modemy, které modulují signál na různé druhy vedení (telefonní apod.)

Linková vrstva zabezpečuje kódování a přenosem informací. Základní jednotkou je datový rámec skládající se ze záhlaví (Header - linkové adresy příjemce, odesílatele a další řídící informace), přenášených dat (Payload - zpravidla packet vyšší - síťové vrstvy) a zápatí (Trailer - kontrolní součet). Typickým představitelem pracujícím na této vrstvě je např. Switch a používá linkový protokol (např. typu Ethernet). Je schopný interpretovat pouze MAC adresy.

Síťová vrstva zabezpečuje přenos dat mezi vzdálenými počítači (WAN) Její síťový packet se skládá ze záhlaví a datového pole. Představitelem síťové vrstvy je Internet Protocol (IP erze 4 nebo verze 6) a z hardware směrovač (Router). Mezi sousedními směrovači je na linkové vrstvě vždy přímé spojení. Směrovač vybalí síťový packet z datového rámce (např. Ethernet) a před odesláním do jiné linky jej opět zabalí do jiného datového rámce poplatnému druhu linky (např. sériová linka). Používá IP (internet Protocol) adresy.
Do třetí vrstvy jsou vrstvy nazývány **nižšími vrstvami.**

Transportní vrstva se věnuje spojení mezi aplikacemi na vzdálených počítačích. Pracuje tak, že předpokládá, že spojení mezi počítači je zajištěno a zcela se spoléhá na služby nižších vrstev a nekomplikuje si život přítomností modemů, směrovačů apod. Jednotkou přenosu je transportní packet skládajícího se opět ze záhlaví a datové části. Nejznámějšími transportními protokoly TCP (Transmission Control Protocol) nebo UDP (User Datagram Protocol)

Relační, Prezentační a Aplikační vrstva mají za úkol udržování a koordinace komunikace, formátování, konverze a zobrazení přenesených dat a přenos informací mezi programy. Pro účely výuky není třeba více popisovat, další informace je možno získat v doporučené literatuře.

Prvky používané v počítačových sítích

HUB - prvek zabezpečující prosté opakování a zesílení signálu vysílaných packetů. Použit byl v prvních typech ethernetových sítí. S nárůstem zásuvek byl postupně nahrazován prvkem s inteligencí - switchem, aby se z kolizní sítě stala použitelná síť bez množství kolizí (viz. výklad přednášky nebo doporučená literatura)
Most (Bridge) - prvek použitý převážně v sítích založených na koaxiálních kabelech, slouží ke spojení segmentů (větví) sítě. Není určen pouze k opakování packetů, ale posílá do vybraného segmentu pouze packety pro určený segment (počítač). Prvek může plnit i bezpečnostní roli - zabezpečení přístupu mezi segmenty.
Přepínač (Switch) - inteligentní prvek využívaný v moderních počítačových sítích. Pomocí různých režimů práce zasílá packety pouze na určená místa a zabraňuje tak kolizím. Novější typy umí pracovat i s VLAN a poslední 2 roky jsou na trhu switche typu Layer3 (pracující i na síťové - třetí vrstvě), které dokáží směrovat packety bez zúžení šířky pásma (a tím rychlosti) do jiných segmentů sítě obvykle v rámci LAN.

Směrovač (Router) - prvek, který je používán jak v sítích LAN, ale převážně jako rozhraní, které rozděluje sítě směrem z LAN do MAN a WAN a pro směrování v rozsáhlých sítích. Pracuje na síťové vrstvě a používá ke směrování např. IP adresy. Slouží zároveň i jako média konvertor tím, že rozbalí rámec z jedné linky a znovu jej zabalí do rámce druhé linky, např. Ethernet - sériová linka, E1 apod.

Parametry digitálních spojů

Šířka pásma - označuje, kolik bitů (kbit,Mbit) lze přenést za jednotku času (obvykle za sekundu) médiem. Hodnota je omezována buď daným druhem média přenosu (metalický, optický kabel, frekvence v prostoru), nebo omezením rychlosti provozovatelem připojení.

Zpoždění - je to doba, kterou potřebuje packet k vykonání cesty z místa odeslání na místo určení. Obecně platí, že čím je větší šířka pásma a čím je méně bodů na trase, tím je zpoždění menší.

Kvalita a spolehlivost přenosu

Kvalita přenosu digitálního spoje je vyjádřena dobou, po kterou spoj vykazuje určitou bitovou chybovost BER (Bit Error Ratio, obvykle 10^{-3} a 10^{-6}) a dobou, po kterou je spoj vyřazen z provozu. Tato doba se obvykle vyjadřuje procentem času měsíce (nebo roku), po které bude spoj vykazovat danou chybovost nebo bude přerušen. Požadovaná kvalita spoje se zadává již při požadavku na spoj a je zřejmé, že požadovaná vyšší kvalita si vyžádá vyšší investice i případně provozní náklady (větší výkon, větší antény apod.) a je tedy třeba již při návrhu zvážit opravdu skutečné potřeby.

Typy přenosu:

Přenos digitálních dat lze realizovat pomocí rozličných technologií a po různých médiích. Digitálními přenosy není možno v současné době chápat pouze přenos "počítačových" dat, ale i přenos dat, ke kterým již počítač není třeba. Jde mi hlavně o hlasové přenosy, které již nemusí být realizovány výhradně po linkách operátorů hlasových služeb, ale prostřednictvím VoIP (Voice over IP) a dalších technologií je již prakticky smazán rozdíl mezi hlasovými a datovými službami, přenos obrazu nevyjímaje.

Obecně tedy jsou přenosy dat realizovány po **metalických vodičích** (viz popis výše), které závisí na technologické úrovni a délce vedení. Například metalické vedení tzv. "poslední míle", tedy od jediného telefonního operátora, který v současnosti vlastní metalické linky až do bytů a firem, může poskytnout při použití analogového modemu rychlost mezi 30 až 50 kbit/s, s použitím ADSL modemu ale už 0,5 až 2Mbit/s dle kvality a délky vedení, které se zjistí prostým změřením útlumu. V rámci budovy firmy lze očekávat, že bude realizace komunikačních vedení provedena formou tzv. "strukturované kabeláže", kategorie 3, 5, 6 či 7, tedy kroucenou dvoulinkou stíněnou či nestíněnou, kde teprve dle potřeby budou zásuvky využity buď pro analogový nebo digitální telefon, či pro počítač. Páteřní linky v rámci nebo mezi budovami nad 100m budou realizovány obvykle **optickým párem vláken** případně **bezdrátovou sítí**, u starších rozvodů pomocí metalických kabelů obvykle se sériovým přenosem. Bezdrátová síť může být realizována pojítky pracujícím ve vyhrazeném - zpoplatněném pásmu, či v pásmu, které je za určených podmínek v tzv. "Všeobecném oprávnění", vydaném ČTÚ, uvolněno pro bezplatný provoz. Definice podmínek, kdy lze používat bezplatně uvolněné frekvence, je velmi složitý a bude vyloženo na přednášce, výčet frekvencí je možno laicky zúžit na pásma: ISM 2,4 GHz dle IEEE 802.11.b a g, a 802.15, v pásmu mezi 5 a 6GHz dle IEEE 802.11.a ETSI HIPERLAN, a v pásmu 10 GHz pro

proprietární technologie (omezený počet definovaých frekvencí, raririta ČR). Materiály k provozování MW spojů ve zpoplatněných kmitočtových pásmech je složité v koncentrované podobě získat v doporučené literatuře, uvádím tedy přehled v tomto materiálu v následující kapitole v plném znění.

Mikrovlnné spoje ve zpoplatněných kmitočtových pásmech

Pro provoz v regulovaných, resp. zpoplatněných pásmech je třeba nejdříve od regulačního orgánu (ČTÚ) zajistit přidělení nevyužitých pracovních kmitočtových "kanálů" v lokalitě instalace, povolení provozu spoje a následně provozovatel spoje hradí regulačnímu orgánu poplatky za využívání přidělených kmitočtových kanálů. Protože přidělování nevyužitých kmitočtových kanálů je ústředně plánováno a je zpoplatňováno, má provozovatel spoje v tomto případě zajištěnu ochranu proti rušení, způsobenému provozem jiných spojů v dané lokalitě. Zde bychom rád upozornil na obecně zažitou a bohužel nesprávnou představu, že provozovatel spoje má současně zajištěnu i ochranu proti zastínění paprsku spoje novými stavbami apod. Tuto ochranu si lze plně zajistit pouze Územním rozhodnutím o ochranném pásmu, vydaném příslušným stavebním úřadem na základě žádosti provozovatele spoje.

Charakteristika nejvyužívanějších provozních kmitočtů radioreléových spojů ve zpoplatněných pásmech

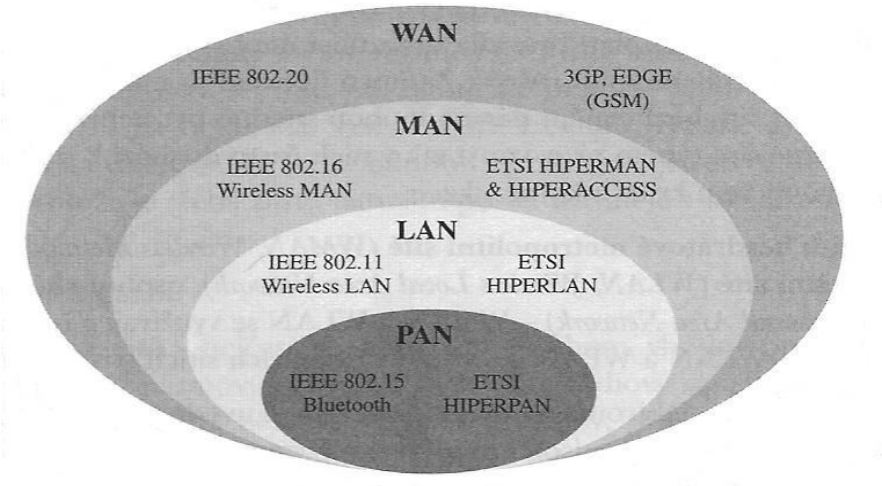
- **3,5 GHz** - je regulované pásmo, určené pro datové a telekomunikační spoje převážně point-to-multipoint (lze ale i point-to-point). Toto pásmo bude z větší části rozděleno mezi několik velkých poskytovatelů veřejných telekomunikačních služeb s celorepublikovou působností (*FWA - Fixed Wireless Access*), kteří si budou samostatně regulovat kmitočtové příděly.
- **7 GHz** - je regulované pásmo, určené pro radioreléové (dále "RR") spoje point-to-point a to zvláště na velké vzdálenosti, z hlediska obsazení kanálů zde vzniká technické omezení pro realizaci spojů v vysokou přenosovou kapacitou
- **13 GHz** - je regulované "univerzální" pásmo, určené pro RR spoje point-to-point
- **15 GHz** - bývalo regulovaným "univerzálním pásmem pro RR spoje, v současné době se vyklízí a nepřiděluje, v budoucnu bude možná část pásma opět uvolněna
- **18 GHz** - je regulované "univerzální" pásmo, určené pro RR spoje point-to-point
- **23 GHz** - je regulované pásmo, určené pro RR spoje point-to-point a vhodné na střední a kratší vzdálenosti a vyšší přenosové kapacity
- **26 GHz** - je regulované pásmo, určené pro datové a telekomunikační spoje převážně point-to-multipoint (lze ale i point-to-point). Toto pásmo je z větší části rozděleno mezi několik velkých poskytovatelů veřejných telekomunikačních služeb s celorepublikovou působností (*WLL - Wireless Local Loop*), kteří si budou samostatně regulovat kmitočtové příděly. Malá část pásma by měla být k dispozici i pro RR spoje point-to-point.
- **38 GHz** - je regulované pásmo, určené pro RR spoje point-to-point, vhodné zvláště pro kratší spoje např. v rámci města a pro vysokokapacitní spoje

Kromě kmitočtového pásma, kde bude spoj provozován, je pro provozovatele velice důležitým parametrem tzv.šířka zabraného pásma, protože právě zabraná šířka pásma je regulačním orgánem zpoplatňována a poplatky jsou jí přímo úměrné. Přesněji řečeno, je zpoplatňován počet zabraných nebo aspoň částečně zabraných standardních kanálů jednotného kmitočtového rastru, stanoveného ČTÚ pro každé kmitočtové pásmo (např. pokud spoj zabírá 3,5 kanálů rastru, poplatek je stanoven za 4 zabrané kanály rastru).

Duplexní spoje potřebují pro svůj provoz v rámci určeného pásma dva kmitočtové intervaly o definované šíři. Tato šíře zabraného pásma je dána jednak požadovanou přenosovou kapacitou spoje (čím větší je přenášená kapacita, tím větší bývá teoreticky i šíře zabraného pásma) a dále způsobem modulace signálu, daném konstrukcí pojítka. Technologicky vyspělejší modulace mohou šířku zabraného pásma výrazně snížit, často však při mnohastavových modulacích je to na úkor snížení dosahu pojítka. Některá pojítka jsou dokonce dodávána s volitelným způsobem modulace signálu a uživatel si pak může vybrat mezi vyšší modulací s levnějším provozem ale kratším dosahem nebo nižší modulací s vyšším dosahem ale dražším provozem.

Pro představu, jak nákladné je pořízení datové konektivity v prostředí krajského města na vzdálenost 5 km (u radioreléových spojů s jednou retranslací), je níže uvedena tabulka. Upozorňuji, že ceny jsou poplatné době vypracování této opory a pronájmem datových okruhů jsou myšleny profesionální garantované symetrické dohledované okruhy.

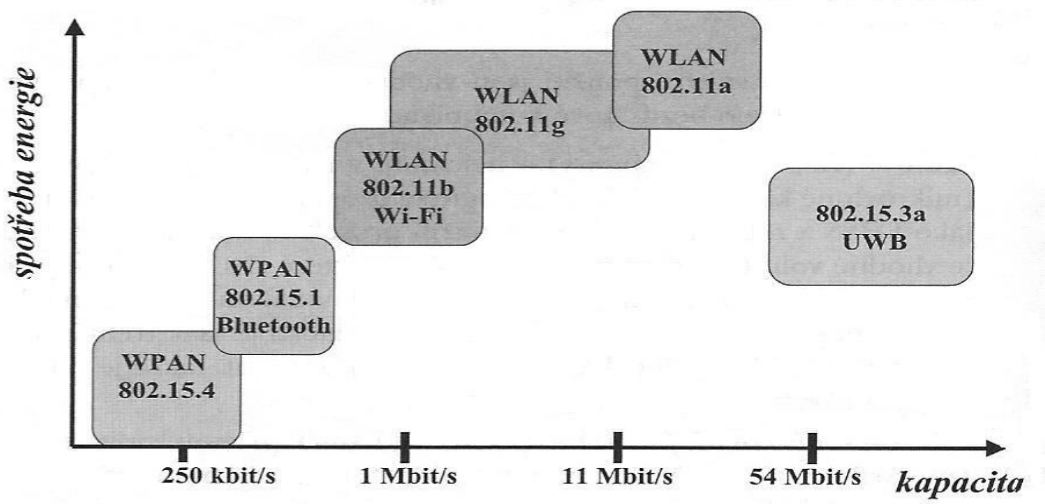
Číslo řešení	Navrhovaný způsob řešení	Rychlost spoje	Předpokládané pořizovací náklady [Kč]	Předpokládané provozní náklady [Kč/rok]
1	kabelové vedení metalické	do 155 Mbit/s	5,000.000,-	do 20.000,-
2	kabelové vedení optické	do 10 Gbit/s	5,000.000,-	do 20.000,-
3	přenos dat pomocí laseru	do 2,5 Gbit/s	50.000,- až 500.000,-	do 20.000,-
4	mikrovlnný spoj (2,4GHz)	do 30 Mbit/s	50.000,-	do 20.000,-
5	mikrovlnný spoj (5,8GHz)	do 36 Mbit/s	60.000,-	do 20.000,-
6	mikrovlnný spoj (10,5GHz)	do 25 Mbit/s	400.000,-	do 20.000,-
7	mikrovlnný spoj v přiděleném pásmu 3,5 až 38GHz	do 34 Mbit/s	150.000 až 1,500.000,-	40.000 až 80.000,-
8	pronájem datového okruhu Ethernet	2 Mbit/s	30.000,-	300.000,-
9	pronájem datového okruhu Ethernet	10 Mbit/s	50.000,-	800.000,-



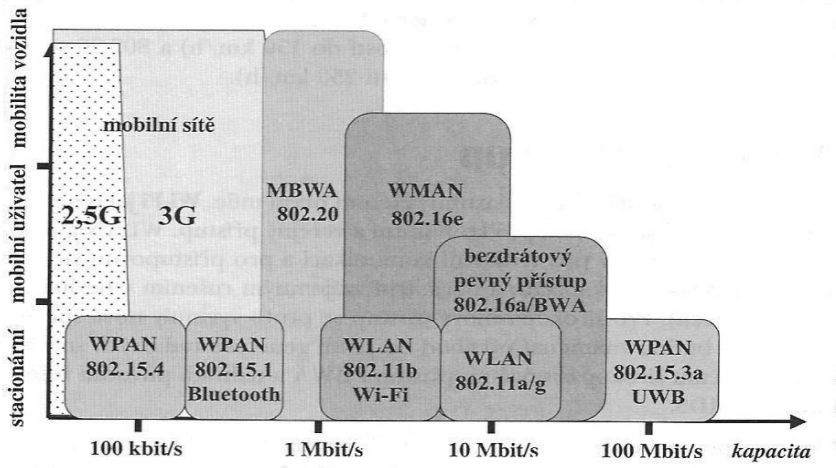
Standardizace IEEE, ETSI - bezdrátové sítě

Struktura výboru IEEE 802 uvedená v souvislosti s pracovními skupinami mající vztah k datovým přenosům

Struktura výboru IEEE 802	
802.1	**Higher Layer LAN Protocols Working Group**
802.3	**Ethernet Working Group**
802.5	**Token Ring Working Group**
802.6	**Metropolitan Area Network Working Group (neaktivní)**
802.8	**Fiber Optic TAG**
802.9	**Isochronous LAN Working Group**
802.11	**Wireless LAN Working Group**
802.14	**Cable Modem Working Group**
802.15	**Wireless Personal Area Network (WPAN) Working Group**
802.16	**Broadband Wireless Access Working Group (BWA)**
802.20	**Mobile Broadband Wireless Access (MBWA)**



Porovnání norem IEEE 802.11 a 802.15 ve vztahu rychlosti a spotřeby energie



Porovnání mobility a kapacity bezdrátových technologií

Doporučená literatura:

1. Shinder, D.L.: Počítačové sítě. Cisco Press 2001, autor.př. SoftPress s.r.o. 2003
2. Pužmanová, R.: Širokopásmový Internet. Computer Press Brno 2004
3. Zandl, P.: WiFi Praktický průvodce. Computer Press Brno 2003

Otázky:

1. Jaké existují topologie počítačových sítí?
2. Jaké typy počítačových sítí znáte?
3. K čemu jsou jednotlivé typy sítí uečeny?
4. Jaké typy médií pro počítačové sítě znáte?
5. Jaké jsou důvody pro přenos dat mikrovlnnými pojítky?
6. V jakých jednotkách se udává šířka pásma digitálních spojů? Uveďte typické hodnoty pro jednotlivé druhy spojů.

5. a 6. Způsoby ukládání dat, databázové systémy, architektura databázových systémů, architektura klient – server

Prakticky vše, co je v počítači uloženo, tedy operační systém, programy i data, jsou uloženy ve formě souborů různého typu v jednom z mnoha file systémů v adresářovém uspořádání v úložišti dat. Tím bývá obvykle pevný disk, média optických mechanik (CD,CDRW,DVD apod.), stále častěji flash média a zanikající diskety. Samostatnou kapitolou jsou DAT pásky a obdobné technologie, příp. opticko magnetická média, která se používají k zálohování a pro běžný přístup k datům jsou používány minimálně. Velké množství dat uložených na těchto médiích, nejsou pro nás životně důležitá, protože je možno je při případné ztrátě naradit s relativně malým úsilím. Toto však neplatí v případě našich vlastních dat, která vytváříme a upravujeme. O tato data se musíme starat a v případě, že tato data máme na vlastním počítači a o zálohování se nestará nikdo za nás (např. určený informatik organizace apod.), stáváme se sami sobě správci dat. A dobrými správci budeme jen v případě, že máme rutinně zvládnuty základy práce se soubory, s adresáři, víme, kde máme důležitá data uložena a zálohujeme vše, co je při případné ztrátě dat zálohovat potřeba, aby bylo možno zálohy v krátké době použít a např. havárie pevného disku PC nám nezpůsobila nenahraditelné škody. Správné vytváření záloh dat není obsahem daného tématu, ale v případě časové rezervy se mu budeme na přednášce více věnovat.

Samotná data mohou být ukládána v neformátovaných souborech základního typu, tedy v textových souborech jak ve volné formě, tak za pomocí různých oddělovačů, je možno použít standardizované formáty, jako např. CSV, které mohu otevřít základními editory, nebo pokročilými tabulkovými procesory, z nichž je možno jmenovat Excel (formát XLS).
V případě psaní textů taktéž mohu data ukládat v jednoduchém formátu, kde použiji pouze základní znaky a kde nejsou řešeny velikosti a typy písma a bez dalších nákladů mohu taktéž použít jednoduché editory, které jsou dnes již nedílnou součástí operačních systémů. Obvyklé je ale pro text použít některý z formátů, který s druhy, velikostí a formátováním umí pracovat a pak je otázkou, zda pracuji v soukromém sektoru nebo ve veřejné správě, kde jsou formáty direktivně určeny standardizací. Nejrozšířenějšími formáty jsou typu DOC (MS Word), RTF apod. Textové editory obvykle mívají konvertory pro převod textu mezi formáty, ale tento převod nebývá obvykle stoprocentně úspěšný. Vhodné je tedy používat formát, se kterým pracuje vaše okolí a nebude mít problém vaše texty přečíst a editovat.

Pokud ale budeme uvažovat o informačním systému, kde budeme pracovat se strukturovanými daty, nelze z mnoha důvodů předpokládat, že by data byla uložena v některém ze zmiňovaných formátů (rychlost přístupu, sdílení apod.). Vývoj v této oblasti prošel různými stupni vývoje. Jednou cestou bylo použití vlastní struktury formátu, který si vytvořil autor informačního systému ke svému obrazu, ale záležitost to byla velmi pracná, a pokud databáze nebyla důsledně ošetřena, stávala se základním problémem celého systému. Druhou cestou bylo použít standardizovaný formát nebo hotový databázový systém. A tím jsem se dostali k databázím, které probereme podrobněji.

Jednoduché databázové formáty

Definice: "**Databáze** je určitá uspořádaná množina informací (dat) uložená na paměťovém médiu. V širším smyslu jsou součástí databáze i softwarové prostředky, které umožňují manipulaci s uloženými daty a přístup k nim. Tento systém se v české odborné literatuře nazývá systém řízení báze dat (SŘBD). Běžně se označením *databáze* – v závislosti na kontextu – myslí jak uložená data, tak i software (SŘBD)".

Typickým představitelem jednoduché databáze je formát DBF. Již při pokusu o zobrazení standardním prohlížečem je prakticky nečitelný a tudíž je zřejmé, že je založen na struktuře a k jeho zobrazení a editaci je nutno znát přesný formát a kompatibilní nástroj. Formát v 80. a 90. letech podstoupil vývoj ve změnách typů atributů a způsobů indexace. Po vytvoření tabulky - databázové struktury se jednotlivé atributy nejprve definovaly a teprve pak bylo možno přidávat , editovat a mazat věty. Tento typ formátu byl oblíben jak od tvůrců nezávislých aplikací v externích programovacích jazycích , tak po uvedení počítačů třídy AT na trh v prostředí Dbase, Foxbase apod. Aplikace postavené na této technologii byly výkonné v závislosti na počtu zpracovávaných vět. Bez použití indexací byly problémem už tisíce vět, se spec. indexy se stav rapidně zlepšil, ale na správu záznamů v počtu milionů již systém stavěn nebyl. Každá tabulka tvořila samostatný soubor, spec. index tvořil další soubor a při použití tzv,."memo", tedy velikostně neomezené položky byl vytvořen další soubor, což při výstavbě velkých systémů způsobovalo problém s velkým počtem otevřených souborů a bylo to velkou zátěží pro tehdejší operační systémy. Tabulky již bylo možno spojovat, ale ještě se nedalo mluvit o typické relaci, což je termín pro generačního nástupce, a to plnohodnotné Relační databáze

Relační databáze

Definice: " **Relační databáze** je databázový systém, který je založen na relačním modelu dat a relační algebře. Data jsou uspořádána do tabulek (relací), nad kterými jsou definovány přípustné operace. Software pro řízení databáze se obvykle nazývá Relational database management system (RDBMS), česky Systémy řízení bází dat (SŘBD). Jazykem pro ovládání databáze je v současné době obvykle SQL, strukturovaný dotazovací jazyk (Structured Query Language)."

Relační databáze je tvořena více tabulkami nebo jinými datovými subjekty, které jsou propojeny společnými vlastnostmi nebo poli, která mají stejnou hodnotu a nachází se v různých tabulkách. Umožňuje pracovat s daty z více tabulek najednou tím, že spojí obsahy odpovídajících si položek. Říkáme, že jsou mezi nimi definovány relace. **Relace** jsou logickou vazbu mezi tabulkami. Musí však platit, že tabulky jsou navrženy strukturovaně. Dále umožňuje uživateli přistupovat k datům propracovanější cestou, bez duplicit údajů, protože data jsou umístěná jen na jednom místě. Použití více tabulek místo jedné zvyšuje rychlost a účinnost ukládání dat. Typickým představitelem je např. MS Access, MySQL, z českých výrobků WinBase.

Typy relací:

1:1 - Tato relace popisuje vztah mezi dvěma tabulkami, ve kterých každý záznam v první tabulce může být přiřazen přesně jednomu záznamu v tabulce druhé. Relaci 1:1 můžeme použít při rozdělení rozsáhlé tabulky, při oddělení části tabulky z důvodů zabezpečení
Příklad: tabulka Osoba obsahuje základní údaje o osobě (titul,jméno,příjmení). Tabulka Prislusnik pak obsahuje pro každý záznam v tabulce osoba jeden příslušný záznam (rodné číslo, adresa domů apod.)
1:N - Jedná se nejčastěji používanou relaci, která popisuje situaci, kdy každý údaj v tabulce může být spojen s mnoha údaji z další tabulky.
Příklad: tabulka Osoba je propojena s tabulkou Zasahy. Jedna osoba pak může být vedena u několika zásahů.
M:N - Relace, ve které se může mnoho záznamů v jedné tabulce vztahovat ke mnoha záznamům v jiné tabulce a naopak.

Příklad : tabulka Osoba je propojena s tabulkou Ukoly. Jedna osoba může mít přiděleno několik úkolů, na druhou stranu na jednom úkolu může pracovat několik osob.

Referenční integrita je nástroj databázového stroje, který pomáhá udržovat vztahy v relačně propojených databázových tabulkách. Definuje se **cizím klíčem**, a to vždy pro dvojici tabulek. Tabulka, v niž je pravidlo uvedeno, se nazývá podřízená tabulka (slave). Tabulka, jejíž jméno je v omezení uvedeno je nadřízená tabulka (master). Pravidlo referenční integrity vyžaduje, aby každý záznam použitý v podřízené tabulce existoval v nadřízené tabulce.

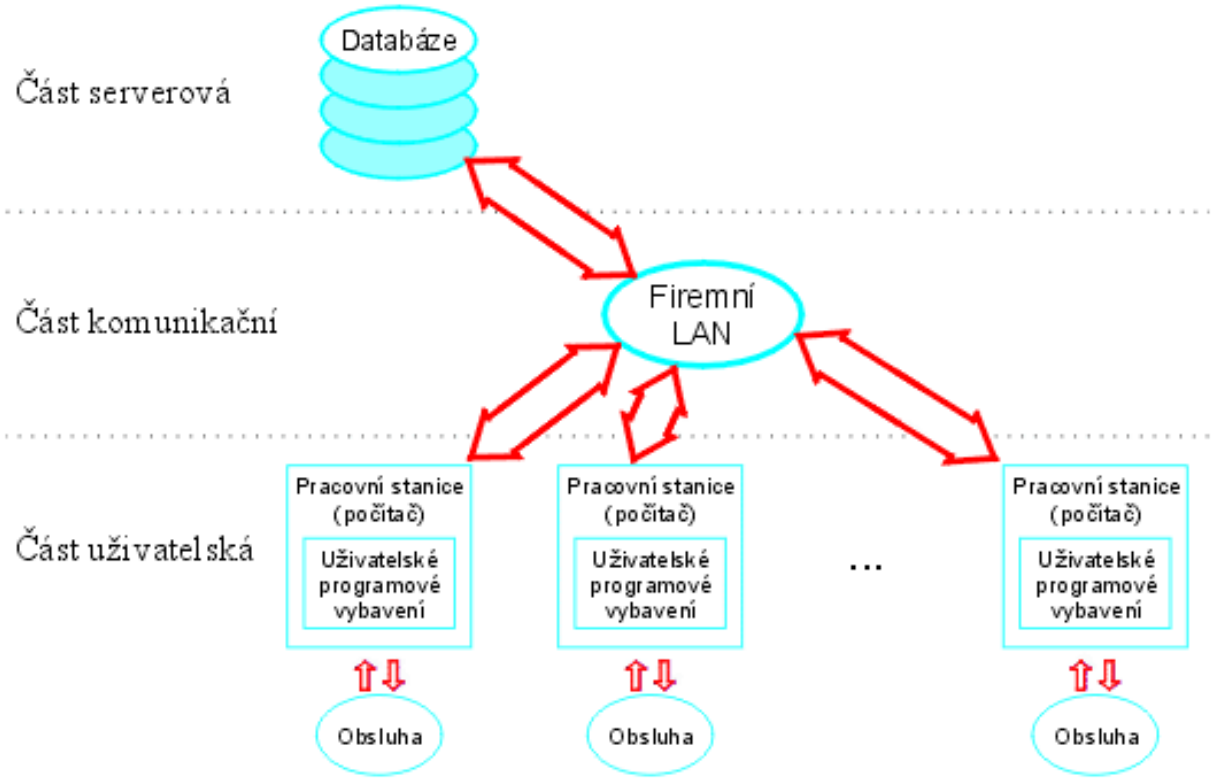
Cizí klíč je sloupec databázové tabulky, který odkazuje na jiný sloupec (jiné tabulky nebo i stejné tabulky). Hodnoty takového sloupce musí být shodné s některou z hodnot v sloupci, ke kterému je klíčem. Vytváří se tak reference – odkaz. Podmínka shody se kontroluje při všech operacích nad databází, což se označuje jako referenční integrita.

Primární klíč je pole nebo kombinace polí, jednoznačně identifikující každý záznam v databázové tabulce. Žádné pole, které je součástí primárního klíče, nesmí obsahovat hodnotu NULL. Každá tabulka může mít definovaný pouze jeden primární klíč. Primární klíč musí mít tři vlastnosti: a) Exkluzivitu (jedinečnost), b) Neměnnost , c) Nenulovou hodnotu .

Typickým příkladem primárního klíče je rodné číslo v seznamu osob, identifikační číslo v seznamu podniků apod. Pokud u záznamu neexistuje žádný přirozený primární klíč, nebo je takový primární klíč příliš složitý, používá se jako primární klíč číslo, které záznamu přidělí automaticky sama databáze. Takové číslo může být pořadové číslo nebo náhodné číslo.

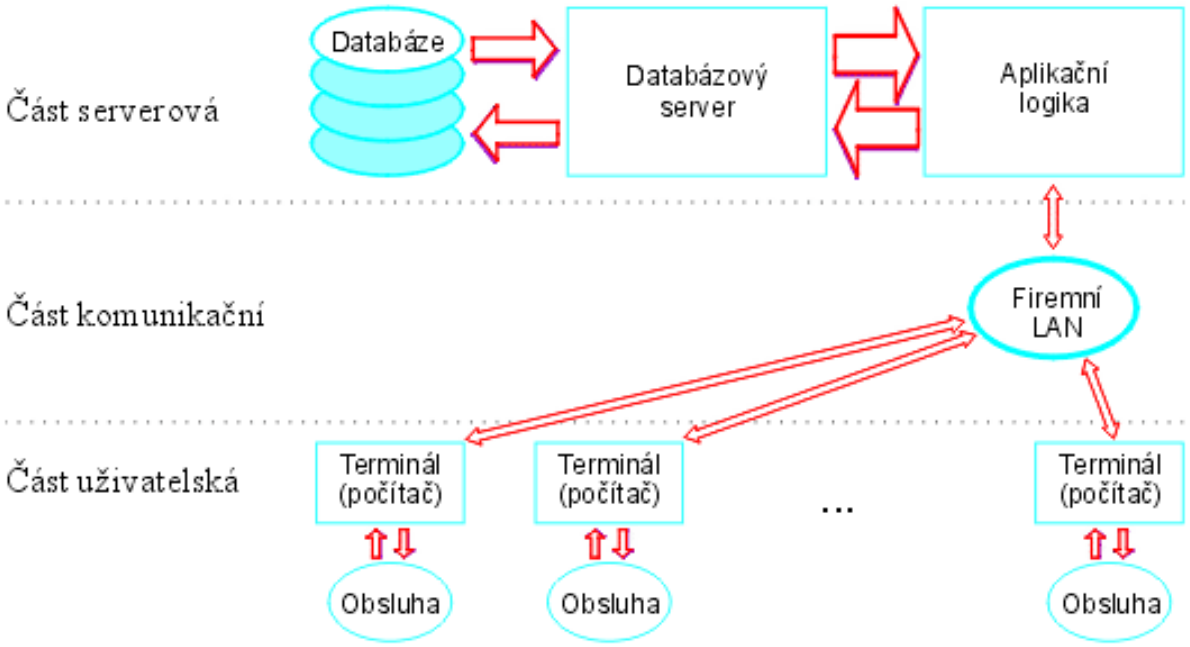
Architektura databázových systémů, architektura Klient – Server

V době, kdy počítače nebyly propojeny pomocí počítačových sítí, bylo standardem, že programy využívaly běžné **souborové databáze**, které byly umístěny na každém počítači. Pokud spolu musely programy komunikovat, bylo to realizováno prostřednictvím exportů a importů obvykle za použití disket či obdobných médií. Příchodem počítačových sítí bylo nutno souborové databáze přesunout na samostatný stroj - server, a programy byly přizpůsobeny pro sítovou práci. Znamenalo to, že všichni uživatelé měli nainstalovaný takto upravený program a uživatelé programů museli obdržet příslušná práva k adresářům a souborům, a to obvykle i práva k zápisu. Tento druh přístupu k datům vysoce zatěžoval počítačové sítě, protože každý z uživatelů přistupoval pro velké množství dat, a teprve tato data zpracovával procesor jejich pracovní stanice. Rychlost práce tak závisela jak na propustnosti počítačové sítě, tak na výkonnosti pracovní stanice. Taktéž je potřeba zmínit problémy, pokud došlo k nekorektnímu ukončení aplikace a záleželo na úrovni zabezpečení konkrétního programu, jak byl schopen se s takovýmito nestandardními stavy vypořádat a nakolik danou situaci musel řešit odborný pracovník - informatik. Práce s daty uloženými na serveru ze vzdálených pracovišť mimo lokální síť, jejíž šířka pásma musela být v řádu desítek Mbit/s, byla prakticky nemyslitelná. Příklad takovéhoto uspořádání je uveden na následujícím obrázku:



Obr. xx - Architektura s využitím souborových databází

Architektura Klient - Server je postavena na logice, kde veškeré operace s databázemi provádí takřka výlučně služba (services) databázový **Server**, který je nainstalován na databázovém stroji, a uživatel na jednotlivých klientských stanicích, tedy **Klient,** má na počítači nainstalovanou pouze klientskou část a vůbec nemusí mít přímý přístup k těmto databázím. Eliminuje se tak potenciální možnost poškození, příp. nechtěné vymazání, působení virů apod. Klient komunikuje pouze se serverovou částí, která zabezpečuje kontakt s databází. Už z prvních vět je zřejmé, že jde o výrazný posun v zabezpečení těchto dat. Nemůže tedy dojít k poškození databáze vinou nekorektních ukončení, uzamčených souborů apod., jak tomu bylo u souborových databází. Další, a to velmi zásadní přínos této architektury je fakt, že klient se serverem komunikuje pouze prostřednictvím úsporných dotazů, které jsou v řádu kbyte a odpadlo tak přesouvání neúnosného množství dat po počítačové síti. Tento fakt má za důsledek možnost přístupu k datům a možnost práce s klientskou částí z místa, které je se serverovou částí spojeno linkou v řádech desítek až stovek kbit/s. Je celkem běžné, že tyto aplikace jsou odladěny na linkách 64kbit/s, což je jeden B kanál ISDN přípojky. Umožňuje to nejenom práci ze vzdálených míst pro zaměstnance (práce z domova, pobočky využívající jeden server v rámci republiky nebo světa), ale i možnost servisních zásahů odborných firem bez nutnosti dojíždění k zákazníkovi. Příklad uspořádání Klient - Server je uveden na následujícím obrázku:



Obr. xx - Architektura Klient - Server

Uživatelskému programu, který pracuje na architektuře s využitím souborových databází se také říká **Tlustý klient**, na architektuře Klient - Server pak **Tenký klient.**

.

Doporučená literatura:

1. http://encyklopedie.seznam.cz
2. http://www.mrp.cz/software/ucetnictvi/ks/porovnani.asp
3. Lacko, L.: SQL Hotová řešení. Computer Press Brno 2003

Otázky:

1. Vyjmenujte druhy úložiště počítačových dat, popište předpokládanou dobu pro bezpečné uchování dat v těchto úložištích.
2. Jaké druhy souborových databází znáte a k čemu se používají?
3. Na jakém principu pracují relační databáze?
4. jaký je základní rozdíl mezi architekturou s využitím souborových databází a architekturou Klient – Server?

7. a 8. Standardy ISVS (Informačního systému veřejné správy), GIS (Geografické informační systémy), UIR-ADR (Územně identifikační registr adres)

Standardy ISVS a metodiky
Standardy ISVS a metodiky jsou soubory pravidel pro výkon odborných činností spojených s vytvářením, rozvojem a využíváním informačních systémů veřejné správy uveřejněné ve Věstníku. Ministerstvo informatiky zajišťuje tvorbu standardů ve spolupráci s orgány veřejné správy, samostatně je vyhlašuje a uveřejňuje ve Věstníku. Standardy ISVS se stejně jako legislativní předpisy a technické normy vyvíjejí. Jejich vývoj ovlivňuje rozvoj poznatků v dané oblasti, postup budování ISVS i změny v právních předpisech a normách. Návrhy nových standardů a zásadní úpravy stávajících standardů jsou vždy projednávány odbornými pracovními skupinami úřadů veřejné správy formou připomínkového řízení. Texty všech platných standardů naleznete na adrese www.micr.cz/dokumenty/koordinace.htm.
Metodické pokyny naleznete na adrese www.micr.cz/dokumenty/metodicke.htm.

Standardy ISVS platné k 31.12.2006
Standard ISVS pro strukturu a výměnný formát digitální technické mapy města - 001/01.02
Standard ISVS pro náležitosti životního cyklu informačního systému - 005/02.01
Standard ISVS pro pověřování k výkonu atestací a pro náležitosti provozu atestačních středisek - 006/03.01
Standard ISVS pro náležitosti procesu a metodiky atestace jakosti produktů - 007/01.02
Standard ISVS k prostorové identifikaci - 008/04.02
Standard ISVS pro zveřejňování vybraných informací o veřejné správě způsobem umožňujícím dálkový přístup - 012/01.02
Standard ISVS pro informační systémy v oblasti personální a platové - 013/04.01
Standard ISVS pro atestace shody informačních systémů veřejné správy se standardy ISVS - 014/01.02
Standard ISVS pro transkripci neběžných latinských znaků do znaků podle kódové tabulky ISO Latin 2 - 015/01.03
Standard ISVS stanovující povinné požadavky na metodiku atestace shody IS se Standardem ISVS pro náležitosti životního cyklu IS - 017/01.01

Ze všech uvedených platných standardů je stěžejní pro naši práci **Standard ISVS k prostorové identifikaci** a tomuto se budeme v následujících odstavcích věnovat, a předstihne tak chronologicky Geografické informační systémy, které mají souvislost s prvním z uvedených standardů - DTMM.

Standardy státoprávního uspořádání:

Již na začátku je třeba upřesnit, že správa po roky používaného Územně identifikačního registru (dále jen ÚIR), která byla spravována Ministerstvem pro místní rozvoj, byla v březnu 2004 protokolárně převedena na Registr sčítacích obvodů (RSO). Registr se v roce 2004 sloučil s Územně identifikačním registrem základních sídelních jednotek Ministerstva pro místní rozvoj.

K průběžné **aktualizaci** registru využívá **administrativní zdroje** dat:

- informační systém katastru nemovitostí, katastrální mapy, ZABAGED, administrativní hranice

- územně identifikační registr adres (je referenčním místem pro číselník ulic a veřejných prostranství)
- adres ze systému evidence obyvatelstva (od roku 2006)
- kromě toho od března 2004 přešla agenda ÚIR-základních sídelních jednotek

dále **vlastní statistické zdroje**:

- statistické zjišťování o budovách u obecních úřadů (jednorázově)
- statistické zjišťování o budovách u stavebních úřadů (čtvrtletně, od roku 2005 měsíčně)
- statistické zjišťování o lokalizaci budov u katastrálních úřadů (ročně, od roku 2006 pololetně)
- podklady od úřadů obcí (průběžně)
- sčítání lidu, domů a bytů.

Úplná historie sledovaných objektů v registru začíná 1. březnem 2001, datem sčítání lidu, domů a bytů a odtud pramení název registru. Probíhá rozšíření datového modelu o plnohodnotnou údržbu adres a koncem roku 2005 byla dokončena datová příprava adresních míst a jejich lokalizace na vchody. Je realizováno propojení statistických budov na Informační systém katastru nemovitostí pomocí jednoznačných identifikátorů budov v České republice a to metodou porovnání přirozeného a alternativního klíče budovy a metodou revize budov nad zbývající množinou nepropojených záznamů.

Prvky standardu (výběr):

Kraj je ve smyslu ústavního zákona o vytvoření vyšších územních samosprávných celků vyšší územní samosprávný celek. Kraj je vymezen výčtem okresů, které jej tvoří. Kraj hl. m. Praha tvoří území hl. m. Prahy jako obce. Kraje celistvě vykrývají území České republiky. Ve smyslu opatření ČSÚ k zavedení klasifikace územních statistických jednotek je kraj územní statistickou jednotkou NUTS 3. Kraj je v kontextu prostorové identifikace prostorovým prvkem charakteru prostorového celku. Je prostorově vymezený hranicí kraje jako vnější hranice okresů resp. hranicí hl. m. Prahy, které jej vytvářejí, tj. na rozlišovací úrovni katastrální mapy.
NUTS - evropská klasifikace územních jednotek pro potřeby statistiky (La Nomenclature des Unités Territoriales Statistiques).

Okres je ve smyslu zákona o okresních úřadech správním obvodem výkonu státní správy okresním úřadem. Okres je vymezen výčtem území obcí (obcemi), které jej tvoří. Pro potřeby Standardu se okresem rozumí i území hlavního města Praha a měst Brno, Ostrava a Plzeň (kde působnost okresního úřadu vykonávají magistráty měst). Takto vymezené okresy pak celistvě vykrývají celé území České republiky. Ve smyslu opatření ČSÚ k zavedení klasifikace územních statistických jednotek je okres územní statistickou jednotkou NUTS 4. Pro tyto potřeby není však okresem hl. m. Praha, ale jsou jimi území působnosti městských částí Praha 1 – Praha 15 v hlavním městě Praze při výkonu přenesené působnosti hl. m. Prahy ve smyslu Statutu hl. m. Prahy, čl. 2. Okres je v kontextu prostorové identifikace prostorovým prvkem charakteru prostorového celku. Je prostorově vymezený hranicí okresu jako vnější hranice obcí, které jej vytvářejí, tj. na rozlišovací úrovni katastrální mapy.

Obec je pro potřeby Standardu území obce ve smyslu zákona o obcích nebo území vojenského újezdu ve smyslu zákona o zajišťování obrany České republiky. Podle zákona o obcích jsou některé obce označovány jako města. V některých směrech specifickou obcí je hlavní město Praha (viz zákon o hlavním městě Praze). Takto vymezené obce pak celistvě vykrývají jednotlivé okresy ve smyslu Standardu a celé území České republiky. Obec je územním samosprávným resp. územněsprávním (vojenské újezdy) celkem základního stupně. Ve smyslu opatření ČSÚ k zavedení klasifikace

územních statistických jednotek je obec územní statistickou jednotkou NUTS 5. Obec je v kontextu prostorové identifikace prostorovým prvkem charakteru prostorového celku. Je prostorově vymezená hranicí obce na rozlišovací úrovni katastrální mapy.

Městská část resp. městský obvod jsou organizační jednotkou města a mohou být zřízeny ve statutárních městech (viz zákon o obcích) nebo v hlavním městě Praze (jen městská část, viz zákon o hlavním městě Praze). Městské části resp. městské obvody nemusí území města plně vykrývat.

Část obce je ve smyslu zákona o obcích evidenční jednotka vytvářená stavebními objekty ve smyslu Standardu (*ve smyslu zákona budovami*) s čísly popisnými nebo evidenčními, přidělenými v jedné číselné řadě (ve smyslu zákona o obcích má část obce ležet v jednom souvislém území, což však v praxi není někdy dodržováno), nebo – v případě, že obec na části členěna není – se za část obce pro potřeby Standardu považuje i celá obec. Taková část obce má název shodný s obcí a obec má pak tedy jedinou část. Z jedné číselné řady jsou číslovány stavební objekty pouze v jediné části obce. Protože se ve smyslu zákona o hl. m. Praze provádí v hl. m. Praze číslování v rámci katastrálních území, jsou pro potřeby Standardu za části obce na území hl. m. Prahy považována katastrální území (nejsou to tedy nadále části obce ve smyslu Standardu k prostorové identifikaci, verze 3.1, které vycházely z územní organizace zveřejněné v Úředním věstníku České republiky). Základní charakteristikou části obce pro potřeby Standardu je, že má vždy samostatné číslování stavebních objektů. Část obce je v kontextu prostorové identifikace prostorovým prvkem charakteru evidenční jednotky (pro evidenci stavebních objektů pomocí čísel domovních), která je vytvářena stavebními objekty. Část obce není vymezena hranicí. V některých případech může obec mít hranici části obce vymezenu. V případě, že obec je sama též částí obce ve výše uvedeném smyslu, je hranicí části obce hranice příslušné obce. Pokud část obce hranici nemá, pracuje se místo s hranicí obvykle s obalovou křivkou stavebních objektů, které část obce tvoří. Ta se však po nárůstu stavebních objektů může měnit.

Základní sídelní jednotka je nejmenší část území státu, za které se provádí základní konečné pořádání výsledků SLDB 2001. Soubor všech ZSJ bezezbytku pokrývá území státu, přičemž každá jeho část přísluší jediné konkrétní ZSJ. ZSJ je tvořena buďto jedním katastrálním územím nebo jeho částí, tzn., že jedna jeho ZSJ nemůže být součástí více katastrálních území. Každá ZSJ je určena její hranicí, která tvoří polygon a definičním bodem, který leží uvnitř (v ploše) tohoto polygonu; ten je tvořen hranicí KÚ, případně částí hranice KÚ a linií, dělící KÚ na rozdílné ZSJ.

Ulice a veřejné prostranství (dále jen UVP) je pro potřeby Standardu taková ulice nebo další veřejné prostranství ve smyslu vymezení v zákoně o obcích resp. v zákoně o hl. m. Praze, které má dopravně-komunikační charakter, tj. zajišťuje přístup ke stavebním objektům nebo pozemkům, nebo vzhledem k nimž jsou číslovány stavební objekty čísly orientačními. V obci nemusí být UVP vymezeny (pojmenovány) – tj. nemusí být zaveden tzv. uliční systém. Uliční systém je však zaveden ve všech městech a větších obcích. V případě obcí s místně odloučenými osadami nebo místně odloučenými samostatnými stavebními objekty, kdy v obci není zaveden uliční systém, jsou tyto odloučené osady resp. odloučené stavební objekty pro´potřeby Standardu též považovány za UVP a za názvy takových UVP se volí pomístní názvy odloučených osad nebo odloučených stavebních objektů. UVP je v kontextu prostorové identifikace prostorovým prvkem jak charakteru prostorového elementárního prvku, tak charakteru evidenční jednotky (pro evidenci stavebních objektů pomocí čísel orientačních). UVP není prostorově vymezena a nemá hranici.

Číslo domovní je souhrnné označení pro číslo popisné a číslo evidenční, je užívané pro potřeby Standardu, není vymezeno žádným právním předpisem. Prostorový identifikátor „číslo domovní“ je vymezen katalogovým listem datového prvku Číslo domovní (viz Katalog jednoduchých datových prvků).

Druh čísla domovního je buď číslo popisné nebo číslo evidenční. Prostorový identifikátor „název druhu čísla domovního“ je pak vymezen katalogovým listem datového prvku Název druhu čísla domovního (viz Standard ISVS Katalog jednoduchých datových prvků).

Parcela je ve shodě s vymezením v katastrálním zákoně pozemek, který je geometricky a polohově určen, zobrazen v katastrální mapě a označen parcelním číslem v rámci katastrálního území. Rozlišují se parcely katastru nemovitostí, jejichž hranice jsou v terénu vyznačeny a parcely evidované zjednodušeným způsobem, jejichž hranice v terénu neexistují. Parcela je v kontextu prostorové identifikace prostorovým prvkem charakteru prostorového elementárního prvku. Parcely ve zjednodušené evidenci se budou s přechodem na nový Informační systém katastru nemovitostí transformovat na parcely katastru nemovitostí.

Adresní místo (stavebního objektu) je takové místo, které lze ve vztahu ke stavebnímu objektu jednoznačně identifikovat adresou stavebního objektu.

Katastrální území Katastrální území je ve shodě s vymezením v katastrálním zákoně místopisně uzavřený a v katastru nemovitostí společně evidovaný soubor nemovitostí. Katastrální území je v kontextu prostorové identifikace prostorovým prvkem charakteru jak evidenční jednotky (pro evidenci parcel pomocí parcelních čísel), tak charakteru prostorového celku. Je vymezeno hranicí katastrálního území na úrovni katastrální mapy.

Parcela je ve shodě s vymezením v katastrálním zákoně pozemek, který je geometricky a polohově určen, zobrazen v katastrální mapě a označen parcelním číslem v rámci katastrálního území. Rozlišují se parcely katastru nemovitostí, jejichž hranice jsou v terénu vyznačeny a parcely evidované zjednodušeným způsobem, jejichž hranice v terénu neexistují.Parcela je v kontextu prostorové identifikace prostorovým prvkem charakteru prostorového elementárního prvku. Parcely ve zjednodušené evidenci se budou s přechodem na nový Informační systém katastru nemovitostí transformovat na parcely katastru nemovitostí.

Adresa stavebního objektu je uspořádaná čtveřice prostorových identifikátorů standardních prvků prostorové identifikace, a to název nebo kód části obce, číslo domovní, název nebo kód ulice a veřejného prostranství, číslo orientační.

UIR-ADR (Územně identifikační registr adres)

Základní údaje:

Za správu a aktuálnost UIR-ADR zodpovídá Ministerstvo práce a sociálních věcí ve spolupráci s obecními úřady tyto úřady udržují registr adres všech stavebních objektů, které mají číslo domovní. Adresy neobsahují žádné údaje o osobách ani organizacích. Česká pošta poskytuje pro adresy platná poštovní směrovací čísla. Registr je využíván pro potřeby státní sociální podpory a úřadů práce. Za spolupráce obcí jsou průběžně doplňovány chybějící adresy, zaznamenávány změny názvů, případně označeny zrušené stavební objekty. Používání registru zajišťuje jednotné a správné psaní názvů a umožňuje kontrolu existence adresy, a tak lze zpřesnit a zrychlit doručování zásilek a zajistit další funkce závislé na přesné a platné adrese. Ministerstvo práce a sociálních věcí dává tento registr k dispozici veřejnosti.

Jak registr UIR-ADR vznikl:

Registr byl vybudován v letech 1997-1999 za spolupráce obecních úřadů, Ministerstva pro místní rozvoj, Ministerstva vnitra, Českého úřadu zeměměřického a katastrálního, Českého statistického úřadu a České pošty s.p. Registr byl původně určen pro potřeby informačních systémů MPSV. Po svém dokončení byl uvolněn i pro ostatní zájemce a rychle se rozšířil mezi desítky uživatelů ze státní správy i mimo ni. Registr prošel od začátku své existence kvalitativním vývojem od původní struktury 1.0 až k současné struktuře 4.2.

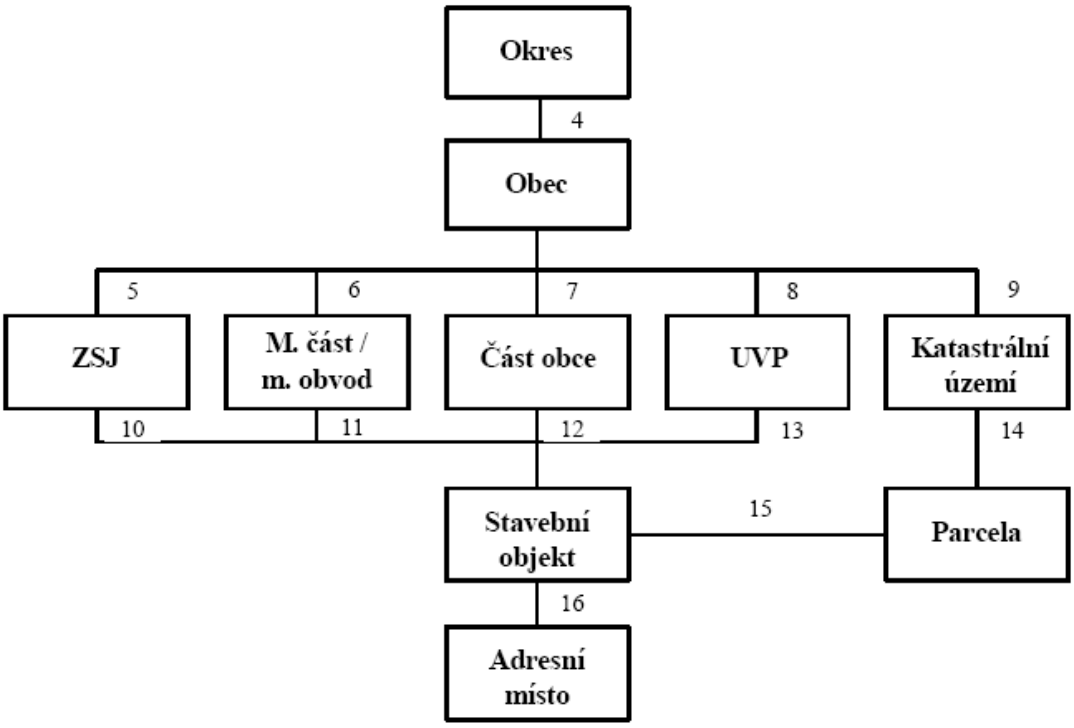
Obsah UIR-ADR:

Registr obsahuje prvky krajů, okresů, obvodů ORP, obvodů POÚ, obcí, pražských obvodů, NUTS4 obvodů, správních obvodů, městských částí/městských obvodů, částí obce, ulic a veřejných prostranství, stavebních objektů, adresních míst, adresních pošt.

Podklady pro číselník ÚIR-ADR:

Číselníky krajů, okresů, obvodů ORP, obvodů POÚ, obcí, pražských obvodů, NUTS4-obvodů a městských částí/městských obvodů jsou do UIR-ADR přebírány z Českého statistického úřadu, číselník správních obvodů z Magistrátu hl. m. Prahy, číselník částí obce z Ministerstva pro místní rozvoj, číselník adresních pošt z České pošty s.p. a číselníky ulic a veřejných prostranství, stavebních objektů a adresních míst jsou udržovány Ministerstvem práce a sociálních věcí na základě hlášení z obecních úřadů. Souřadnice adresních míst jsou do UIR-

Oficiální schéma UIR pro území ČR (mimo hl. m. Prahu)



Doporučená literatura:

1. www.micr.cz/dokumenty/koordinace.htm.
2. www.micr.cz/dokumenty/metodicke.htm.

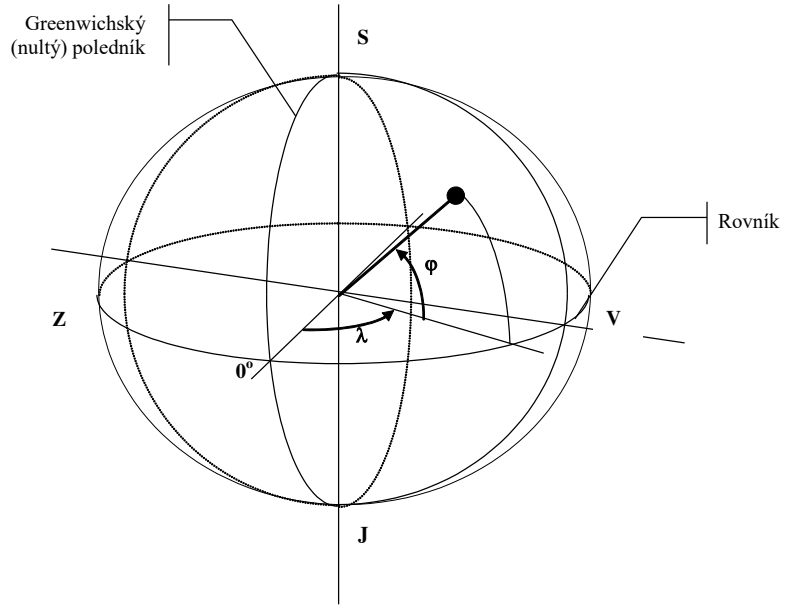
Otázky:

1. Proč je důležitá standardizace?
2. Vyjmenujte základní prvky standardizace ISVS prostorové identifikace (místopisu)
3. Jaký je rozdíl mezi ÚIR a ÚIR-ADR?
4. Jaký je rozdíl mezi Základní sídelní jednotkou a Katastrálním územím?

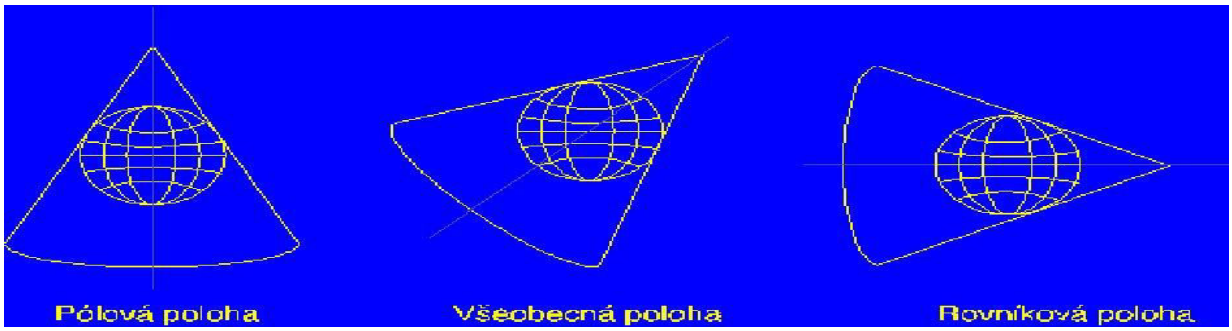
Geografické informační systémy

Souřadné systémy

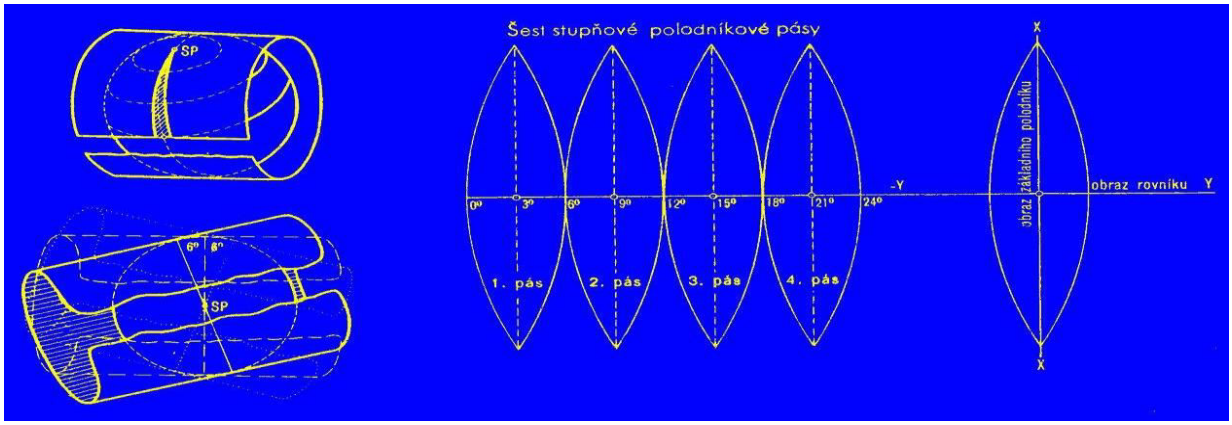
Geografický souřadnicový systém (v principu sférický), poloha bodu na zemském povrchu je udávána pomocí zeměpisné šířky φ (latitude) a zeměpisné délky λ (longitude).



WGS 84



Promítání na kužel – např.: S-JTSK



Promítání na válec – např.: S42, Gauss-Krügerovo

Základní principy

Většina objektů a jevů reálného světa se vyskytuje na některém místě zemského povrchu (např. strom, dům, řeka) nebo má vztah k některému místu na zemském povrchu (občan má někde trvalé bydliště, výrobek byl vyroben v určité továrně). Zároveň se tyto objekty vyskytují v daném prostoru společně s mnoha dalšími objekty a navzájem se ovlivňují (např. hlukem ze silnice jsou postiženi obyvatelé v domech do určité vzdálenosti, komín zamoří zplodinami určité území, prosperita prodejny závisí mimo jiné i na její poloze a množství potenciálních zákazníků v okolí). Proto znalost umístění a vzájemných prostorových souvislostí mezi objekty je velmi významná a může sehrát důležitou roli v řadě oborů lidské činnosti, od návrhu umístění jaderné elektrárny až po návrh obchodní sítě a vyhodnocování její úspěšnosti.

Prakticky to znamená, že v našich datech v počítači musíme mít zaznamenáno obojí současně, tj. jak vlastní údaje o objektu, tak údaje o jeho poloze. Tomuto typu dat říkáme geografická (nebo prostorová) data a počítačovému systému, který umožňuje ukládat a využívat taková data říkáme geografický informační systém, zkráceně GIS.

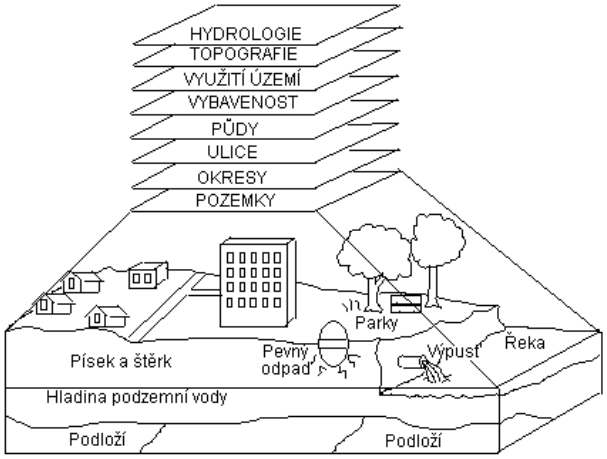
S jednoduchými prostorovými daty může pracovat i mnoho široce používaných počítačových programů, jako jsou databáze, tabulkové procesory, statistické programy nebo programy pro technické kreslení (CAD). V čem se tedy liší GIS od těchto programů?

... co není GIS...

1. GIS není jenom počítačový systém na tvorbu map, přestože může vytvářet mapy nejrůznějších měřítek, zobrazení a barev. GIS je nástroj pro analýzu.

2. Hlavní výhoda GIS spočívá v tom, že vám umožní určovat prostorové vztahy mezi geografickými objekty zobrazenými na mapě.

3. GIS neukládá mapy v klasickém slova smyslu; ani neukládá nějaký konkrétní obraz nebo pohled na geografickou oblast. Místo toho ukládá GIS data, ze kterých lze potřebný pohled vytvořit, takovým způsobem, aby vyhovoval konkrétnímu účelu. Viz obr.



Vrstvy GIS (nahoře) v. Realita (dole)

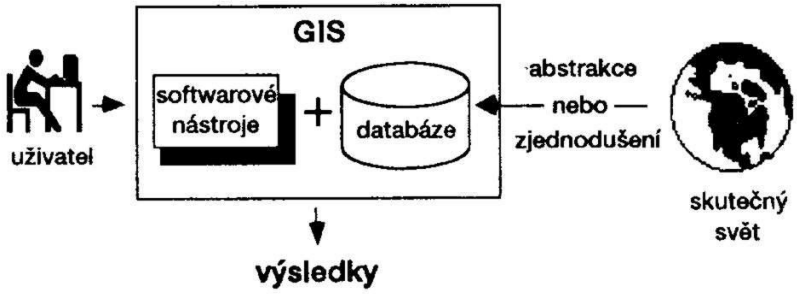


Schéma práce s GIS

Podporované datové formáty

Vektorová data :

ARC/INFO coverages (atributy uložené v INFO formátu)
PC ARC/INFO coverages (atributy uložené v DBASE formátu)
Mapové LIBRARIAN layers (knihovny vrstev)
ArcStorm library layers
CAD soubory (*.dgn, *.dxf, *.dwg)
Spatial Database Engine (SDE)
Geodatabase a Personal Geodatabase

Rastrová data :

GRID (ARC/INFO), TIFF TIFF/LZW compressed, LEICA IMAGINE, BSQ, BIL and BIP, Sun rasterfiles, BMP, JPEG (rozšíření JPEG image), MrSid, Image catalogs

Prvky vektorových dat :

Points, Arcs, Polygons, Label points, Nodes Routes, Regions, Annotation (popisy)

Tabulková data :

INFO, dBASE, Oracle, MS Access,RDBMS přes SQL, XML, Textové soubory (oddělené tabulátorem nebo čárkou) a další….

Doporučená literatura:

1. www.arcdata.cz , publikace Arc Revuespol ARCDATA Praha s.r.o.
2. http://support.esri.com/
3. http://www.cuzk.cz/
4. http://www.esri.com/
5. http://www.cagi.cz/

Otázky:

1. Jaký druh základní standardizace využívá GIS?
2. Co si představujete pod zkratkou GIS?
3. Co není GIS?
4. Jaké souřadnicové systémy znáte?

9. Bezpečnostní zásady při ochraně dat, zásady a konkrétní postupy při bezpečném přístupu k informacím

Proč potřebujeme bezpečnost ?

Na počítačových sítích je dnes dostupné opravdu vše. Vývojem komunikačních prostředků je možno propojit prakticky veškeré databáze, které nás zajímají a začínáme si zvykat na to, že na on-line informacích jsme závislí. Informace je ceněný artikl a zvlášť některá data pochopitelně jsou v ohrožení zájmovými skupinami či jednotlivci a přibývá pokusů o průnik do počítačových sítí a informačních systémů. Každým rokem se ztrojnásobí přiznané průniky, a to připomínám, že se jedná o slovo „přiznané“. Ze statistik vyplývá, že největší slabinou je uživatel.

Proto vzletná otázka v úvodu může vyprodukovat třeba i celou knihu odpovědí. Důležité je ale vybrat takové odpovědi, které jsou důležité pro posluchače, tedy běžné uživatele. Ale jak jsme si již v předchozích kapitolách řekli, i uživatel se v dnešní době stává správcem svých dat například proto, že používá přenosný počítač v terénu, vlastní počítač pro přístup do firemní sítě apod. Pokud se jedná o firemní data, tam je za nastavení jejich bezpečnosti odpovědný obvykle profesionál – informatik dle zpracované bezpečnostní politiky firmy, ale již nemůže zajistit, že se prostřednictvím vašich přístupových údajů nedostane k datům někdo nepovolaný. Z toho je zřejmé, že v bezpečnostní politice musí být stanoveny také jasné povinnosti pro uživatele, aby k takovýmto stavům nemohlo dojít. Nejprve si tedy odpovíme na otázky, jak se má chovat uživatel, jaké bezpečnostní rizika mu hrozí a pokud v přednášce zbude čas, seznámíme se v obecné rovině s typy útoků a hrozbami, kterým musí čelit správci informačních systémů.

Heslo dne: **„Systém je tak bezpečný, jak bezpečné je jeho nejslabší místo“**.

Jak už jsem si řekli, nejslabším místem bývá mnohdy právě uživatel. Ten svou práci začíná spuštěním počítače a přihlášením se. Ale kam se přihlašuje? To je ta správná otázka. Pokud pracuje na odděleném počítači, ověřuje jeho přihlášení operační systém (OS). Pokud je připojen ve firemní LAN, neměl by ho ověřovat OS, ale řadič domény či jiné LDAP ověření. Už zde je moment, který může uživatel ovlivnit jednoduchým přepnutím v okně přihlášení. Samozřejmě, je možné namítnout, že pokud mě neověří „vyšší instance“, nedostanu se k datům, ale v případě moderních OS i při odpojení od firemní sítě s sebou nese v přenosném PC informace o připojení k doméně a jsou v jistých případech techniky, jak heslo zjistit, zvlášť pokud je k počítači fyzický přístup. Pokud se ověřuje u PC, ohrožuje data umístěná na PC. Pokud se ověřuje u jiné instance, ohrožuje data pod její správou.

Jak zvolit správné heslo? Toto je klasická otázka, na kterou je stále stejná odpověď: v žádném případě nepoužívat standardní jména a hesla, která přiděluje systém, nepoužívat jména, příjmení, datumy narození, čísla pojištění, průkazů, SPZ vozidel vlastních ani blízkých členů rodiny (včetně rodinných mazlíčků – zvířátek) a to ani jejich kombinace, obrácená pořadí apod.. Jsou to první údaje, která jsou při pokusu o uhádnutí hesla použity. Hesla by měla být dostatečně dlouhá (alespoň 8 znaků) a je nutno kombinovat písmena malá i velká a čísla. Důležité je ale taktéž zásada heslo z důvodu zapomenutí nikam nezaznamenávat. Lístečky s hesly nalepené na monitoru počítače jsou trestuhodným příkladem.. Další zásadou by měla být výměna hesla po určité době, za zmínku stojí i možnost zabezpečení přenosných počítačů biometrickými prvky (otisk prstu apod.), což se stává v současné době již standardní výbavou. Největší ohrožení nastává v případě připojení PC na internet. Při lokálním připojení, např. z domova nebo mobilními prostředky je nutné, aby byl počítač chráněn buď HW, nebo alespoň SW firewallem (je dnes již součástí moderních OS). Samozřejmostí je pochopitelně

aktualizovaný a plně funkční antivirový program, v dnešní době důrazně doporučuji kombinaci s ochranou proti spyware (nejvhodnější je kombinace alespoň dvou druhů, z nichž alespoň jeden kontroluje na pozadí zápis do registru), dále update operačního systému – aplikace bezpečnostních záplat. A poslední a velmi důležité upozornění: Nikdy nepřistupujte k bankovním účtům z neověřených počítačů (Internet Banking apod.). Vystavujete se tak vysokému riziku vyzrazení přístupového jména hesla a zneužití služby!! Konkrétní důvody a vysvětlení tohoto odstavce bude důkladně provedeno při výuce.

Připojení k Internetu ve firemní síti by v současných podmínkách již nemělo být přímé, ale prostřednictvím Proxy serveru a v případě, kdy to není možné, povolit přímý přístup jen pro konkrétní služby (Access listy, porty a konkrétní IP adresy). Mezi základní znalosti uživatele musí patřit vlastnosti protokolů používaných při práci s Internetem ve vztahu k bezpečnosti. Pokud odesíláme směrem do internetu data standardním protokolem HTTP, tato data jsou jednoduše „odchytitelná“ a čitelná a není možno touto cestou provádět přihlášení do jiných systémů, obzvláště to platí, pokud používáte své „oblíbené“ heslo do všech systémů – snad nejhrubší uživatelská chyba. Existuje protokol HTTPS, který je již zabezpečen obvykle 128 bitovou šifrou SSL a i v případě použití jednoduchého protokolu je obvykle možno přihlášení provést se SSL nebo obdobným zabezpečením. Při opuštění pracoviště (toaleta, jednání, oběd) je dobrou zásadou před odchodem uzamknout počítač, protože pokud nejste schopni kontrolovat, kdo má k počítači přístup, je možné, že by na vaše zalogování mohla neoprávněná osoba zneužít data, informační systém, přečíst vám poštu a způsobit jinou škodu.

Zásady a doporučení, jak se má chovat správce k podnikové síti, by přesáhlo rámec přednášky, ale protože některé z těchto činností jsou shodné s činnostmi, které je třeba provádět i pro jednotlivé počítače a mohou mít pro vás význam, budou zmíněny jen bodově a dle časových možností vysvětleny na přednášce.

- Používat aplikační proxy a firewally, systémy na detekci/prevenci průniků (IDS/IPS)
- Oddělit servery od uživatelů, VLAN, Firewall
- Přístup do podnikové sítě zvenčí zabezpečit prostřednictvím VPN za použití IPSec, autorizovat HW prostředky (např. RSA apod.)
- Servery dostupné z Internetu umístit do DMZ
- Zneaktivnit nepoužívané zásuvky LAN, vazba na MAC adresu
- Důsledně používat antivirové systémy na serverech, stanicích, bránách, email serverech, permanentně aktualizovat antivirové služby
- Aplikovat bezpečnostní záplaty, pravidelně scannovat celou síť
- Zamezit provoz zbytečně spuštěných aplikací (služeb), znát komunikační nároky aplikací (porty TCP, UDP)
- Používat doménová pravidla, LDAP, pokud je to možné šifrovat provoz
- Logovat firewally, routery, kritické aplikace a kontrolovat logy se zaměřením na scannovaní otevřených portů a útoky na ně
- Pravidelně zálohovat – online, pokud je to možné udržovat pravidelně dvě aktivní kopie
- Prověřovat hesla uživatelů - útok typu pokus omyl
- Šifrovat a autentizovat WLAN

Doporučená literatura:

1. Prosise, Ch., Mandia, K. Počítačový útok. Detekce, obrana a okamžitá náprava. Computer Press Praha 2002.
2. Dostálek, L., Kabelová, A. Velký průvodce protokoly TCP/IP a systémem DNS. Computer Press Praha 2000
3. Pužmanová, R.: Širokopásmový Internet. Computer Press Brno 2004
4. Zandl, P.: WiFi Praktický průvodce. Computer Press Brno 2003

Otázky:

1. Jaké jsou zásady pro tvorbu hesla?
2. Jaký je rozdíl mezi počítačovým virem a spyware?
3. Je bezpečné se do informačních systémů přihlašovat protokolem HTTP?
4. K čemu slouží Proxy server?
5. K čemu slouží Firewall?
6. Co jsou to bezpečnostní záplaty operačních systémů?

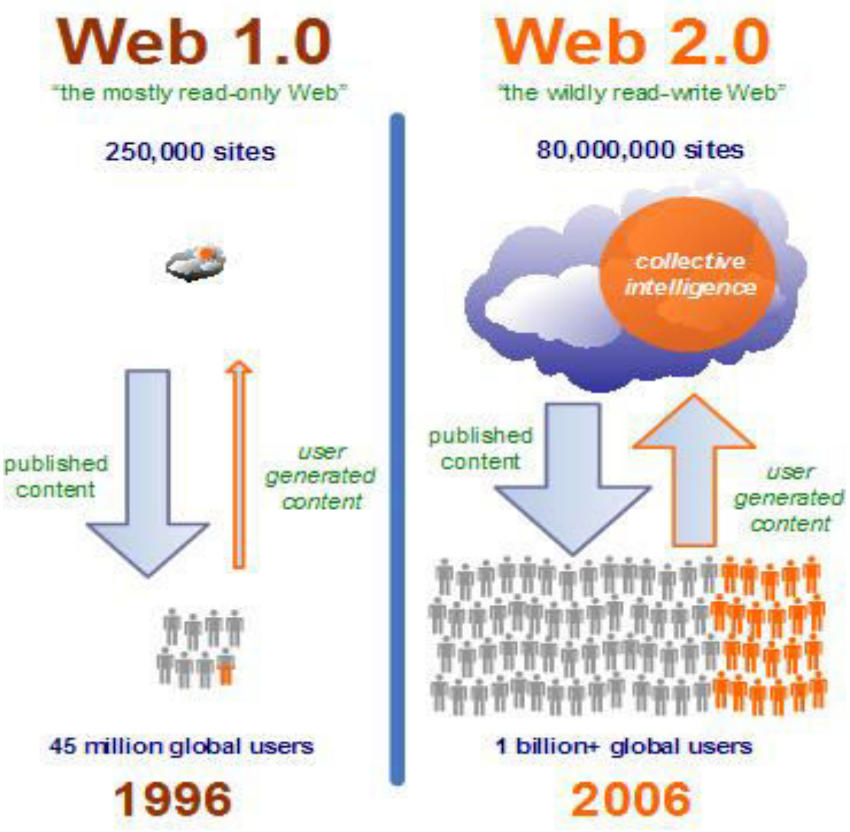
10. a 11. Využití Internetu jako zdroje dat, popis funkcionality, přístupy, Veřejně dostupné zdroje informací.

Jak už bylo řečeno, na počítačových sítích je dnes dostupné opravdu vše. Pokud chápu Internet jako síť, která spojuje ostatní sítě, stává se Internet prakticky neomezeným zdrojem dat. A může být zdrojem dat veřejně dostupných, i neveřejně dostupných. Je to jen otázka zabezpečení přístupu. Obvyklé je že informační systémy sestávají z veřejné a neveřejné části, kde neveřejná část bývá dále rozdělena na část, která zobrazuje data určené pouze pro oprávněné subjekty a část, které je určena pro správu dat. Než si některé takovéto zdroje konkrétně popíšeme, řekneme si něco o historii a popisu funkcionality Internetu.

Historie Internetu

Vznik Internetu se datuje začátkem šedesátých let v USA. Jako odpověď na vypuštění družice Sputnik Sovětským svazem v roce 1957 založila americká vláda v rámci Amerického ministerstva obrany Úřad pro pokročilé výzkumné projekty. Tím chtěla zajistit Spojeným státům prvenství ve vědě a technologii aplikované ve vojenské praxi. Hlavní myšlenkou při zakládání tohoto úřadu byla decentralizace počítačové sítě, která nebude mít ani jeden "kritický bod" zničitelný jediným jaderným útokem, tedy vytvořit síť, která by propojovala nejdůležitější vojenské, vládní a akademické počítače a neměla žádnou centrálu, takže by byla schopna funkce i při výpadku jednotlivého uzlu. Za finanční podpory Pentagonu se pustili do budování decentralizované sítě univerzity MIT a UCLA. Již v roce 1968 byla zprovozněna první kompletní síť pojmenovaná jako Arpanet. O dva roky později se rozrostla na 15 uzlů. O rok později to již bylo 37 zapojených počítačů. Jako hlavním využitím sítě se ukázala výměna dat.Tím byl také vymyšlen e-mail. O rok později, tedy v roce 1973 se připojili další univerzity, ale ne americká, nýbrž anglické, to bylo signálem, že decentralizovaná síť je trefou do černého a má budoucnost. V roce 1974 byl vytvořen protokol TCP/IP . Hlavními tvůrci této sady byli Vinton Cerf a Robert Kahn. Prvé testy se začaly provádět v roce 1975. V roce 1977 proběhla demonstrace práce sítě ARPANET pod řízením internetových protokolů. TCP protokol v roce 1978 autoři rozdělili na dva, na vlastní TCP a na IP (Internet Protocol). Do sady mezi hlavní internetové protokoly byl zařazen ještě UDP (User Datagram Protocol) a ICMP (Internet Control Message Protocol). Vinton Cerf zavedl jméno nové počítačové sítě - Internet - s velkým počátečním písmenem.V roce 1983 byl TCP/IP určen jako hlavní protokol pro přenos dat v Internetu. Následujících 9 let se Internet neuvěřitelně rozrostl. V roce 1986 byla založena páteřní síť NSFNET dosahující rychlosti přenosu až 56 kit/s(v roce 1988 zvýšena na 1,544 Mbit/s (T1), v roce 1991 pak na 44,736 Mbit/s (T3)), zahrnující 5 superpočítačových středisek,. Vznikl sytém Gopher, který byl předchůdce WWW (world wide web) . V roce 1990 byl předveden první WWW server. Tato střediska podnítila doslova explozi počítačů nově připojených do Internetu. Pro něj se dnes hojně používá obecná zkratka ISP, neboli Internet Service Provider. Připojovaly se další země, mezi nimiž v roce 1991 i Česká republika. Roku 1992 došlo k založení společnosti zabývající se historií, vývojem, trendy a etikou Internetu. Počet hostitelských počítačů v Internetu překročil jeden milión. Od roku 1993byl Internet průlomový, do internetu se totiž začali připojovat komerční subjekty. Nejdříve počítačové firmy, později i jednotliví jedinci. V roce 1993 se zakládá instituce, která udržuje adresářové a databázové služby účastníků Internetu, provádí registraci doménových jmen a přidělování adres. K Internetu se připojil i Bílý dům a členové americké vlády včetně prezidenta. Na Internetu již můžeme sledovat audio i video vysílání prvních televizních a rozhlasových stanic. Připojují se obchodní společnosti a média, které doté doby neměly s počítači nic společného a nastává informační exploze.V roce 1994 slaví Internet 25. výročí.

Roku 1995 se služba WWW dostává na první místo v počtu přenesených dat. Mnoho firem, operujících na Internetu se stává veřejně proslulými. Internet se stává stále více součástí běžného života. a to hlavně zejména prostřednictvím elektronické pošty. Začalo být zcela běžnou záležitostí uvádět na své vizitce též adresu internetové elektronické pošty, www stránky společností nebo i vlastní. Budoucnost se bude stále více zaměřovat na interaktivní práci uživatele s Internetem a vytváření Internetu uživatelem.



Rozdíl mezi Internetem a intranetem:

Intranet je uzavřená skupina navzájem komunikujících počítačů pracující obdobnou technologií, kterou využívá Internet. Jinak jej můžeme nazvat také jako lokální síť. Intranet může být pomocí serveru napojen do Internetu Internetová síť nemá vlastníka, jedná se o veřejnou síť, která není na nikom závislá. Nemá centrální počítač. Pokud "vypadne" jeden počítač, stane se pouze to, že když zavoláte jeho adresu, nedostanete odpověď, ale síť běží dál. Síť se skládá z tzv. domén a každá doména má svého providera - poskytovatele připojení. Uživatel může zažádat o připojení k Internetu u libovolného providera, aniž by došlo k nějakým omezením.

Základní protokoly a služby Internetu a intranetu

Protokol TCP (Transmission Control Protocol) umožňuje vytvořit mezi dvěma hostitelskými systémy oboustranné propojení garantující bezchybný přenos posloupnosti paketů v tomtéž pořadí, v jakém byly vyslány**.**

Protokol UDP (User Datagram Protocol) pracuje nad protokolem IP podobně jako TCP. Je vybaven slabším mechanizmem pro zotavení z chyb, zato jednodušším způsobem vysílá a přijímá pakety přes síť. Obvykle se využívá pro streamy videa, přenos zvuku (např. VoIP telefonie).

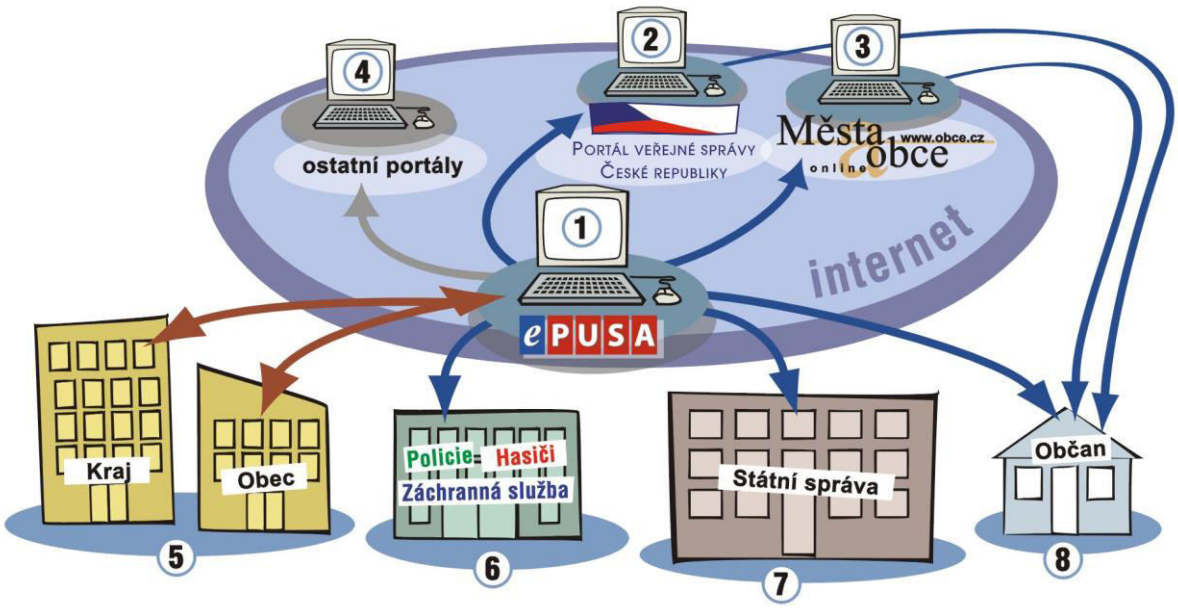
Protokol ICMP (Internet Control Message Protocol) se zabývá pakety obsahujícími chybová, příkazová nebo informační data. Tak například program **PING**, testující průchodnost propojení k danému cíli, využívá tento protokol.

Systém doménových jmen DNS (Domain Name server) ustavil pro internetové počítače hierarchicky organizovaná doménová jména a vzájemnou konverzi mezi IP adresami a doménovými jmény. Bylo definováno šest velkých domén nejvyšší úrovně: EDU (education), GOV (government), MIL (military), COM (commercial), ORG (organization) a NET (network resources). Tato skupina byla rozšířena i o národní domény. Pro USA byla zavedena doména US, SRN DE, Česká republika CZ apod.

Veřejně dostupné zdroje v Internetu

V záplavě informačních zdrojů přístupných prostřednictvím Internetu zmíním jen čtyři, které mají souvislost se studijním oborem. Je na posluchačích, aby samostudiem vyhledali další informační systémy, o kterých je možno odborně diskutovat.

- **ePUSA** – elektronický portál územních samospráv
  - opravdu se nejedná o elektronický polibek. Jde o typického představitele informačního systému přístupného z Internetu. Níže je na obrázku nastíněn pohyb dat. Výklad k IS bude proveden na přednášce.



1. Elekronický portál územních samospráv **2.** Portál veřejné správy ČR **3.** Města a obce OnLine **4.** Ostatní portály **5.** Krajské a obecní úřady **6.** Integrovaný záchranný systém a krizové řízení **7.** Státní správa, ministerstva **8.** Občan – domácí uživatel

- **TRINS** (transportní informační a nehodový systém)
  - TRINS poskytuje prostřednictvím svých středisek nepřetržitou pomoc při řešení mimořádných situací spojených s přepravou či skladováním

nebezpečných látek na území České republiky. Pracuje ve třech stupních podpory:

- 1. stupeň :Telefonická porada
- 2. stupeň Porada v místě zásahu (nehody)
- 3. stupeň Praktická pomoc v místě zásahu (nehody)

- **DOK**
  - DOK je informační systém, jehož hlavním úkolem je podpora vybraných činností v oblasti krizových situací v dopravě. Nebezpečné látky, odpady, přeprava nebezpečných věcí, databáze nebezpečných látek. mezinárodní předpisy RID/ADR/ADN , kterými se řídí přeprava nebezpečných věcí se v České republice.
- **IS ARGIS** (Státní správa hmotných rezerv)
  - IS ARGIS je Informační systém plánování civilních zdrojů, který provozuje Státní správa hmotných rezerv (dále SSHR). Jedná se o nástroj informační podpory hospodářských opatření pro krizové stavy v oblasti zajišťování věcných zdrojů. Jeho hlavním cílem je pomoci orgánům krizového řízení od úrovně obecních úřadů s rozšířenou působností (dále ORP), přes úroveň krajských úřadů až po ministerstva a ostatní ústřední správní úřady při plnění povinností uložených:

    - zákonem č. 241/2000 Sb. o hospodářských opatřeních pro krizové stavy,
    - zákonem č. 240/2000 Sb. o krizovém řízení a
    - vyhláškou SSHR č. 498/2000 Sb. o plánování a provádění hospodářských opatření pro krizové stavy, v platném znění.

    Existuje i tzv. off-line verze prohlížení statických dat pojmenovaná **Hádes.**

Doporučená literatura:

1. Dostálek, L., Kabelová, A. Velký průvodce protokoly TCP/IP a systémem DNS. Computer Press Praha 2000
2. Pužmanová, R.: Širokopásmový Internet. Computer Press Brno 2004
3. Zandl, P.: WiFi Praktický průvodce. Computer Press Brno 2003
4. www.nic.cz – DNS
5. www.lupa.cz – seriál o historii Internetu Vladimíra Vrabce
6. www.epusa.cz

Otázky:

1. Kdy a jak vznikl Internet?
2. K čemu slouží Internet?
3. Jaké základní protokoly a služby Internet využívá?
4. K čemu slouží DNS?
5. Co je DHCP a k čemu slouží?
6. Vyjmenujte důležité veřejně přístupné informační systémy dostupné z Internetu.

12. a 13 Zásady tvorby informační podpory, analýza problému, návrh struktury dat I. a II.

Obor, který studujete, není specializací pro vytvoření profesionálního tvůrce informačního systému, programátora nebo informatika. Během vaší práce se ale můžete setkat se situacemi, kdy se od vás bude očekávat analytická práce a definice problému, který je potřeba zpracovat formou databáze nebo informačního systému.
Ty tam jsou doby pionýrských začátků, kdy programátorovi byl zadavatelem nastíněn problém, který je třeba řešit a on byl uvržen do problematiky, kterou byl nejprve nucen v rámci možností nastudovat, pak vytvořit analýzu, databázové struktury a nakonec napsat aplikaci, tedy vytvořit program. Teprve při prvním předvedení práce zadavatel pochopil, že od systému chtěl něco jiného a bylo velmi problematické dosavadní práci zahodit a začít lépe, systémově. Lépe ve smyslu toho, že nebyla zanedbána analýza, a do procesu musel vstoupit odborník toho oboru, kterého se projekt týkal, a tento odborník úzce spolupracoval jak na analýze, tak při tvorbě databázových struktur, i samotného programu – zde samozřejmě pouze v rámci struktury menu a funkcionality. Od té doby se mnohé změnilo, vývojové firmy mají vlastní analytiky a propracované systémy, existují i SW nástroje pro správu návrhů informačních systémů (tzv. CASE - Computer Aided Software (System) Engineering). Ale jak známo, vše je o penězích, a pro vyřešení některých problémů není možno povolávat nákladné odborné týmy, nebo je věc tak specifická, že analýzu problematiky musí zpracovat zadavatel. Sám jsem byl svědkem výroků programátorů – „Dejte mi písemně zpracované zadání, já vám vytvořím programu“. Pak ale jakákoliv chybička, nejasnost nebo opomenutí v zadání je chybou zadavatele, programátor sdělí, že postupoval přesně podle zadání a začínají komplikace.

Proto si **ve dvou přednáškách nastíníme zásady této práce a na konkrétním příkladu z oboru, který bude vytvářen interaktivně se studenty přímo během přednášky. Nejprve provedeme analýzu zadaného problému a poté budeme navrhovat datové struktury a dle časových možností i referenční integrity struktury dat**.

K samostudiu vyjmenuji pouze hlavní etapy budování informačního systému a dále odbornou literaturu, ze které je možno čerpat. Vzhledem ke specifice tématu nebudou v tomto materiálu zadány otázky, ale tyto budou stanoveny na konci přednášky.

Hlavní etapy budování informačního systému

1 Analýza

- problémů
- procesů
- uživatelských požadavků a potřeb

2 Návrh

- struktur
- tvorba uživatelského rozhraní
- tvorba dokumentace
- testování

3 Implementace a integrace

4 Provoz, údržba, zajištění kvality

Doporučená literatura:

1. Habr, J., Vepřek, J. Systémová analýza a syntéza : zdokonalování a projektování systémů. 2. přeprac. vyd. Praha : SNTL, 1986.
2. Kučerová, H. Projektování informačních systémů. Sylaby ke kurzu. Praha: Vyšší odborná škola informačních služeb, 2004
3. Adamec, S., Horný, S., Rosický, A. Projektování informačních systémů. Praha: Vysoká škola ekonomická, 1997.
4. Chlapek, D., Řepa, V., Stanovská, I. Techniky a nástroje vývoje informačních systémů. Praha: Vysoká škola ekonomická, 2000.
5. Řepa, V. Analýza a návrh informačních systémů. *1. vyd. Praha: Ekopress, 1999. 403 s. ISBN 80-86119-13-0*

Otázky:

1. Vyjmenujte čtyři hlavní etapy budování informačního systému.
2. K čemu slouží analýza a proč je pro návrh informačního systému stěžejní?
3. Podle jakých kritérií volíme pro informační systém databázový systém?

14. Legislativa v oblasti přístupu k informacím a ochrany dat

Právní zabezpečení ochrany dat

Rozvoj informatiky přinesl potřebu koncentrace velkého množství různých údajů ze všech oblastí lidské činnosti. Data mají obecně větší hodnotu, než samotné informační systémy určené k jejich zpracování. Informace jsou neustále zhodnocovány a upravovány tak, aby byly aktuální a co nejvíce užitečné.

Propojením často samostatně nevýznamných údajů z více databází může dojít k takové situaci, kdy by zneužití dané informace (její zveřejnění, zničení, poskytnutí někomu, kdo by z ní mohl mít prospěch) mohlo výrazně poškodit určitou osobu či organizaci. Často totiž jde o data týkající se obchodních údajů firem či osobních údajů osob (registry obyvatel ministerstva vnitra, údaje zdravotních pojišťoven údaje o bankovních kontech, o finančních pohledávkách nebo i údaje sociální z různých statistických průzkumů či reklamních kampaní). Proto musí být zajištěna důsledná ochrana dat, a to jak technická (hierarchické přístupy k datům pomocí hesel, kódování dat, fyzické zabezpečení pracoviště), tak i právní – formou přijetí příslušných zákonných norem.

Právní předpisy

S informačními systémy nějakým způsobem souvisí hlavně tyto obecné právní předpisy: ***občanský zákoník, trestní zákon, autorský zákon, zákon o ochraně osobních údajů v informačních systémech, zákon o ochraně topografií polovodičových výrobků, obchodní zákoník, zákon o ochraně státního tajemství, zákon o elektronických komunikacích, zákoník práce a konečně i sama Listina základních práv a svobod***, jež je součástí naší **Ústavy**. Tyto zmiňované právní předpisy se týkají informačního systému organizace.

Porušování autorských práv

Z hlediska pracovněprávní a autorskoprávní ochrany organizace je třeba, aby byla mezi programátorem a zaměstnavatelem předem uzavřena smlouva (pracovní nebo zvláštní autorská), v níž obě strany definují programy takto vzniklé jako autorské dílo konkrétních autorů, stanoví rozsah oprávnění obou stran (souhlas autora s distribucí, případně závazek o vzdaní se šíření jím samým), výši odměny nebo způsob jejího určení (jako prémiovou složku platu nebo jako samostatnou odměnu, např. podle výše prodeje či využívání).
Z hlediska ochrany proti nelegálnímu užívání programů v organizaci – což se děje zejména užíváním programů zaměstnavatele k soukromým účelům, užíváním nelegálně získaných programů na počítačích zaměstnavatele, provozováním programů na více počítačích, než bylo ve smlouvě dohodnuto, zasahováním do programu, dalším prodejem nebo jiným poskytnutím programu třetí osobě i dalšími způsoby – jde o dva aspekty: občanskoprávní a trestní.

Stávající praxe orgánů činných v trestním řízení při zjištění porušování autorských práv v organizaci spočívá ve vznesení obvinění proti osobě, která skutek spáchala. Jestliže není zjištěna, je stíhána osoba, která odpovídala za provoz programů v organizaci. Jestliže taková osoba neexistuje nebo takové úkoly nemá jednoznačně v pracovní náplni, je stíhán statutární zástupce odpovídající za celou organizaci nebo její autonomní část.

Porušování předpisů o ochraně osobních údajů

Veškeré úpravy v oblasti ochrana osobních údajů u nás mohou vycházet z Listiny základních práv a svobod, kde je v článku 10 výslovně řečeno, že „každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“. Ochrana zájmů o fyzických osobách – občanech, zejm. údajů o zdraví, občanské cti a soukromí, vyplývá přímo z § 11 občanského zákoníku. Podle tohoto ustanovení jde o „nedělitelnou součást celkové fyzické a psychicko-morální integrity osobnosti“. V případě zveřejnění nepravdivých nebo zavádějících údajů může fyzická osoba podat soudní žalobu na základě § 19 občanského zákoníku.

Co se týká ochrany údajů o právnických osobách, vychází právní úprava z obchodního zákoníku. Jde zejména o § 17 obsahující ochranu obchodního tajemství. Za obchodní tajemství jsou považovány veškeré skutečnosti obchodní, výrobní či technické povahy (obchodní knihy, kalkulace, technologie, speciální software), které mají alespoň potencionální hodnotu, nejsou běžně dostupné a podnikatel má výlučné právo obchodním tajemstvím nakládat, zejm. udělovat svolení k užití. V případě průmyslového a duševního vlastnictví (patenty, ochranné známky, software) lze užít k tomuto svolení licenční smlouvu (§ 508). Pokud trvají skutečnosti podle § 17, je právo k obchodnímu tajemství časově neomezené. Právní ochrana poskytuje ve smyslu § 53 tyto prostředky:

- odstranění závadného stavu,
- poskytnutí přiměřeného zadostiučinění, a to i finančního,
- náhradu škody,
- vydání bezdůvodného obohacení.

Zákon o ochraně osobních údajů v informačních systémech č. 256/1992 Sb.

Tento zákon vznikl právě za účelem ochrany dat a informací. Zákon stanoví odpovědnost právnických a fyzických osob, které přichází do styku s informačními systémy. V úvodu zákona jsou vymezeny některé pojmy, např.:

Osobní údaje jsou informace, vztahující se k určité konkrétní osobě. Fyzická osoba, o níž dané údaje vypovídají, se nazývá dotčená osoba.

Za **informační systém** zákon považuje „funkční celek zabezpečující systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací“. V podstatě tedy nejde jen o samotný výpočetní systém, databázi a odpovídající programové vybavení, ale i o pracovníky, kteří se stávají součástí takového informačního systému.

Provozování informačního systému představuje soubor komplexních činností: shromažďování, zpracování, poskytování a rušení informací. Poskytování informací se v této souvislosti nazývá **informační službou**. Zpracování informací spočívá v podstatě v udržování aktuálnosti údajů prostřednictvím jejich modifikace, doplňování a automatizovaného zpracování. Likvidace informací představuje v podstatě jejich trvalé znepřístupnění, a´t už formou výmazu nebo dokonce likvidací fyzického nosiče údajů. S daným informačním systémem přichází do styku řada osob. Zákon definuje provozovatele informačního systému, uživatele informačního systému a zprostředkovatele.

Provozovatelem informačního systému je fyzická nebo právnická osoba, zabezpečující zpracovávání údajů a zpřístupňování informačních služeb. Je zároveň nositelem práv a povinností spojených s provozováním informačního systému.

Uživatel využívá informace z informačního systému, a to buď přímo nebo prostřednictvím informačních služeb. Ke styku uživatele s provozovatelem může sloužit **zprostředkovatel**.

Ten může dále zajišťovat sběr informací pro provozovatele. Sběr informací musí probíhat tak, aby nedocházelo k narušování práv a svobod občanů.

Provozovatel musí požádat o registraci informačního systému u zvlášť k tomu zřízeného orgánu (§ 24 ZOÚ), s výjimkou systémů určených výhradně pro vnitřní potřeby provozovatele nebo systémů pracujících pouze se zveřejněnými informacemi. Při ukončení činnosti musí být tento orgán informován bezodkladně provozovatelem. U nás nebyl prozatím tento orgán zřízen.

Na fyzické osoby, které v rámci svého pracovního nebo obdobného poměru nebo v rámci své funkce či smluvní činnosti mají přístup k danému informačnímu systému, se vztahuje povinnost mlčenlivosti. Tato povinnost platí i po ukončení pracovního poměru či výkonu smluvní činnosti.

Ochrana zatím může probíhat pouze soudně, důkazy se postižená strana musí zajistit v podstatě sama. Jelikož ovšem provozovatel není povinen vpustit cizí osoby do podniku ani poskytnout podklady, může velice dobře odstranit veškeré důkazní stopy.

Další trestné činy

U počítače stejně jako u jiné movité věci může jít o trestný čin krádeže, zpronevěry, podvodu, podílnictví, zatajení věci, jakož i poškozování cizí věci. Poměrně častý je výskyt deliktů podle ustanovení § 249 – neoprávněné užívání cizí věci. Většinou však dochází ke dvěma typickým projevům počítačové kriminality: počítání na počítači zaměstnavatele a v návaznosti na to prodávání programů, které vznikly v návaznosti v rámci pracovního poměru, jiným uživatelům pod vlastní hlavičkou.Tady je však vhodné rozlišovat nevýdělečné počítání v pracovní době, mimo pracovní dobu a výdělečné počítání.

Poškození a zneužití záznamu na nosiči informací

Podle § 257a odst. 1 je postihován, „kdo v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch získá přístup k nosiči informací a a) takových informací neoprávněně užije, b) informace zničí, poškodí nebo učiní neupotřebitelnými nebo c) učiní zásah do technického nebo programového vybavení počítače“.

Některé související zákony a nařízení vlády ve spojitosti s ochranou (osobních) dat

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy.
Zákon č. 480/2004 Sb., o některých službách informační společnosti
Nařízení vlády č. 173/2006 Sb., o zásadách stanovení úhrad a licenčních odměn za poskytování informací podle zákona o svobodném přístupu k informacím.

Ochrana dat

Existuje mnoho cest, kterými může uživatel ohrozit počítačový systém a získat přístup k jeho informacím. Z tohoto důvodu vzniká potřeba na ochranu dat. Samozřejmě každá taková snaha na ochranu dat se nepříznivě projeví především v zatížení výkonu počítače a v nemalé míře také znepříjemní práci obsluze.

Předmět ochrany dat

Obecně lze problémy počítačové bezpečnosti rozdělit do sedmi klíčových oblastí:

1. **Zajištění soukromí** - každý jedinec nebo organizace musí mít možnost volby, kdy a s kým bude sdílet svá data.
2. **Zajištění povoleného přístupu** - Definice práv explicitně pro každého uživatele buď

individuálně, nebo pomocí skupin, případně kombinací obou metod.

3. **Zajištění integrity** -žádnému jedinci nesmí být zabráněno v použití informace proto, že někdo jiný informaci zničil.

4. Zajištění přístupu ke službám - žádnému jedinci nesmí být zabráněno v použití informace proto, že někdo jiný poškodil prostředky, zajišťující k této informaci přístup.

5. Omezení možnosti zneužití - privilegovaným uživatelům nesmí být umožněno zneužít důvěry k získání neautorizovaného přístupu k datům a prostředkům nebo k oprávněnému udílení přístupu jiným osobám.

6. Identifikace problémů - administrátor musí být v případě prolomení bezpečnosti stanovit konkrétní příčinu a určit co nejpřesněji rozsah škody.

7. Zajištění bezpečnosti - uživatelé musí mít jistotu, že komunikují se skutečně důvěryhodným systémem.

Legislativa:

- ***občanský zákoník***
- ***trestní zákon***
- ***autorský zákon***
- ***zákon o ochraně osobních údajů v informačních systémech***
- ***zákon o ochraně topografií polovodičových výrobků***
- ***obchodní zákoník***
- ***zákon o ochraně státního tajemství***
- ***zákon o elektronických komunikacích***
- ***zákoník práce***
- ***Listina základních práv a svobod***
- ***Zákon č. 365/2000 Sb., o informačních systémech veřejné správy***
- ***Zákon č. 480/2004 Sb., o některých službách informační společnosti***
- ***Nařízení vlády č. 173/2006 Sb., o zásadách stanovení úhrad a licenčních odměn za poskytování informací podle zákona o svobodném přístupu k informacím***
- ***Usnesení vlády ČR č. 624/2001***

Doporučená literatura:

3. Čada, O.: Operační systémy. Praha, Grada, a.s. 1994.
4. Donát J.: Hlídejte si je!. CHIP, 1995, č.5, str. 46 - 49
5. Matyáš, V.: Ochrana dat v síti PVT. ComputerWorld, 1995, č.24, str.7
6. Kmoch, P.: Informatika a výpočetní technika. Praha, Computer Press 1997.
7. http://www.micr.cz/

Otázky:

1. Jakým zákonem je v ČR chráněn počítačový program?
2. Co je OEM program a jaký pro něj platí omezení?
3. Jakým způsobem jsou v ČR chráněny osobní údaje?
4. Co víte o UV 624/2001?