Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

POZIADAVKY ORGANIZÁCIE NA BEZPEČNOSŤ IKT

prof. Ing. Pavol Pavol Horváth, PhD.

Slovenská technická univerzita
pavol.horvath@stuba.sk

KPMG
cutting through complexity™

ŠTRUKTÚRA PREZENTÁCIE

- **Štruktúra IKT v organizácii**
- **Bezpečnosť IKT v organizácii**
- **Prevádzka, údržba a zálohovanie IS organizácie**
- **Metódy a prostriedky riadenia projektov**
- **Návrh informačných systémov**

ŠTRUKTÚRA IKT V ORGANIZÁCII

- **Útvar IKT v organizácii sa obvykle delí na :**
- **Technickú a systémovú obsluhu**
  - **Správa LAN a pripojenia do internetu – správa IP adries**
  - **Správa (údržba) technických komponentov počítačového systému - PC servery, dátové úložiská**
  - **Správa operačných systémov**
  - **Správa databáz – nastavovanie, monitorovanie**
- **Správu jednotlivých aplikácií – subsystémov IS**
- **Útvar pre analýzu a vytváranie špecifických výstupov z IS**
- **Ochrana a bezpečnosť prístupu k IS organizácie**

OCHRANA A BEZPEČNOSŤ PRÍSTUPU K IS

- **Spracovaný „Bezpečnostný projekt“**
- **Určený bezpečnostný manažér organizácie**
  - **Monitorovanie incidentov prístupu k dátam IS, vrátane zabezpečenie účinnej ochrany (analýza rizík)**
  - **Ochrana pred zanesením vírusov, trójskych koňov a iných škodlivých programov**
  - **Nasadenie antivírových a antispamových programov**
  - **Definícia a klasifikácia citlivých údajov v organizácii a realizácie usmernenia s ich nakladaním**
  - **Spracovaný havárijný plán informačného a počítačového systému**

BEZPEČNOSŤ IKT V ORGANIZÁCII

- **Otázku bezpečnosti IKT je možné rozdeliť do 4 oblastí**
  - **Dátová**
  - **Sieťová**
  - **Prevádzková**
  - **Fyzická**

BEZPEČNOSŤ DÁT

- **Bezpečné uloženie a ochrana pred zneužitím**
  - **Pre bezpečné uloženie je optimálne použitie Diskových polí RAID**
  - **Zálohovanie v inej (geograficky vzdialenej) lokalite**
  - **Ochrana pred zneužitím treťou stranou šifrovaním virtuálnych serverov a ich diskového priestoru**
  - **Ochrana prístupu – prístupové práva**
  - **Správa hesiel**
  - **Spôsob prideľovania hesiel**

SPRÁVCA DATABÁZY

- **Zabezpečuje plynulý chod celého DBS, ale aj systémových programov a základné činnosti v správe údajov**
- **Správca (administrátor) môže vytvárať, pridávať, meniť a vymazávať objekty v každej databáze a má prístupové práva do všetkých databáz, ktoré sú vytvorené v danom systéme**
- **Úlohy adminstrátora tvorí - inštalácia databázového systému, správa diskového priestoru pre ukladanie údajov a databáz**
- **Spravuje a monitoruje diskový priestor, pamäti a prepojenia jednotlivých serverov navzájom, autorizuje identifikáciu hesiel a prístupových práv, zálohuje a obnovuje databázy, diagnostikuje systémové problémy a vylaďuje SQL Server tak, aby dosahoval čo najlepšie výkony**

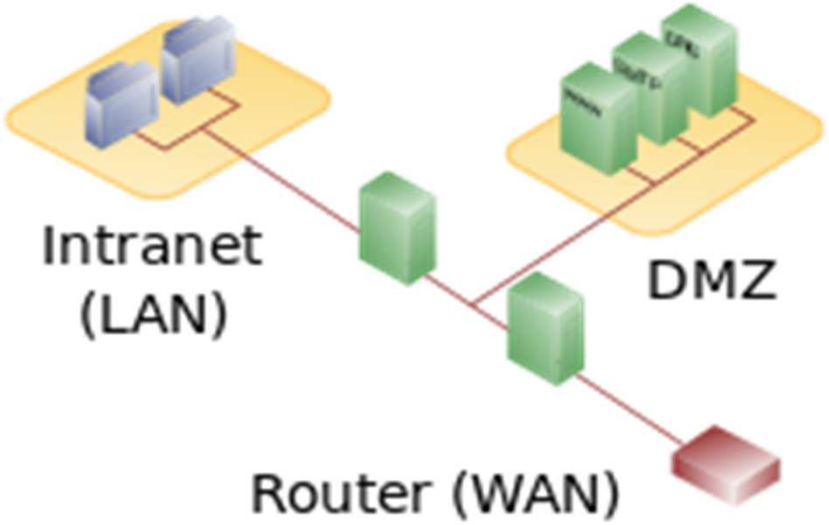
SPRÁVCA PODSYSTÉMU IS

- **Zabezpečuje správu jednej alebo viacerých aplikačných programov IS napr. správy personálneho a mzdového podsystému**
- **Správca podsystému IS (aplikácie) určuje prístupové práva pre konkrétnych používateľov, stanovením ich rolí napr. či niektorí používatelia majú prístup k údajom a funkciám aplikácie a keď tak ku ktorým**
- **Úlohou správcu aplikácie je aj sledovanie požiadaviek používateľov na zmeny dátových štruktúr, tlačových výstupov alebo štruktúr na obrazovke zo strany používateľa**
- **Monitoruje diskový priestor aplikácie, ako aj všetky systémové hlásenia a prípadné chyby rieši so správcom databázy**

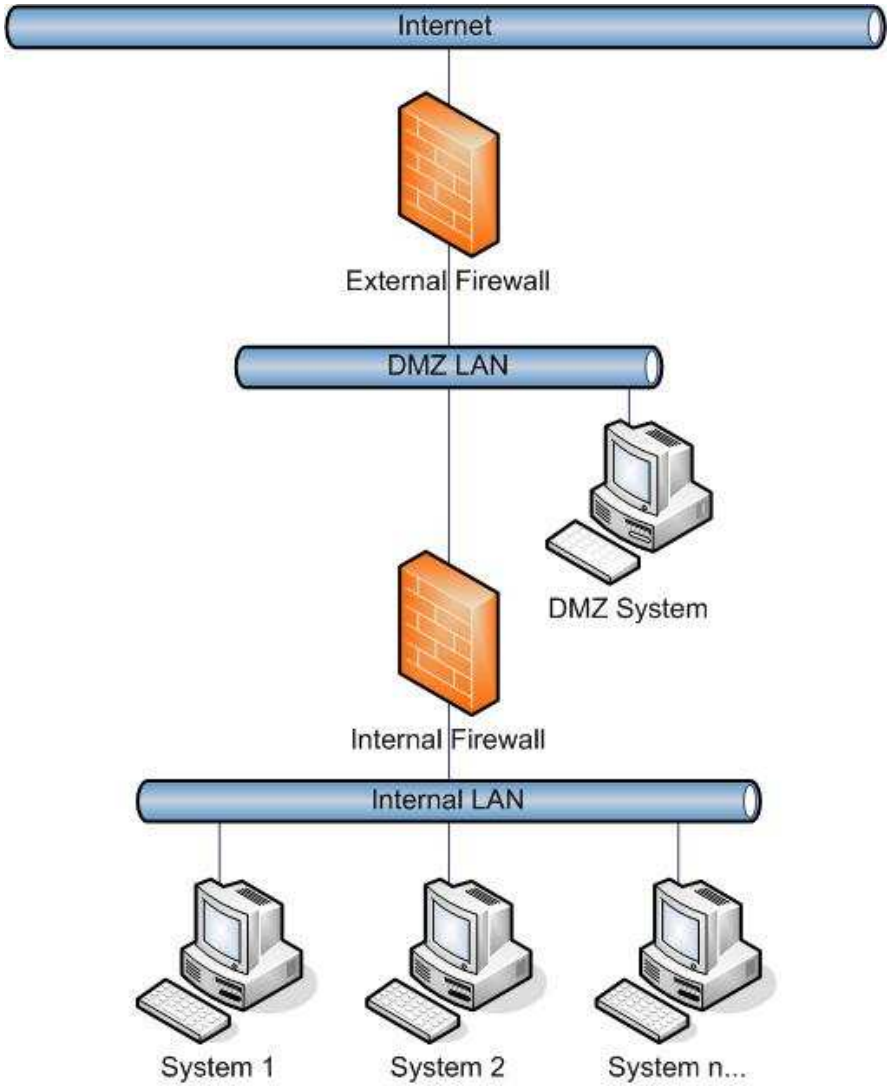
BEZPEČNOSŤ IKT V ORGANIZÁCII

- **Sieťová bezpečnosť:**
  - **použitie virtuálneho firewalu alebo použitím vlastného fyzického zariadenia**
  - **Bezpečná komunikácia cez šifrovaný tunel s protokolmi IP Sec Open VPN, alebo SSL**
  - **Vyvažovanie záťaže - Load balancing**
  - **Systémy na odhaľovanie útokov a detekciu zraniteľnosti systému**
  - **Web aplikačný firewal na webové služby**

- **prístup k akejkoľvek službe poskytovanej používateľovi cez sieť LAN, alebo WAN, napr. prístup do databázy musí chránená cez firewall**
- **za firewall do tzv. DMZ – demilitarizovanej zóny sa umiestňujú dôležité servery napr. databázový server, dátový sklad, niekedy aj mailový server**
- **na obr. je jednoduchá schéma s 2 firewallmi, jeden chráni prístup z internetu a druhú z intranetu**



- **DMZ (anglicky *demilitarized zone*) je fyzická nebo logická podsieť, ktorá je z bezpečnostných dôvodov oddelená od ostatných zariadení**
- **V DMZ sú umiestnené služby, ktoré sú k dispozici väčšinou z celého internetu**
- **Účelom DMZ je pridanie ďalšej bezpečnostnej vrstvy v LAN**
- **To znamená, že prípadný útočník získá prístup len k zariadeniam, ktoré sú v DMZ, ale zvyšok LAN – napr. dôležité databázové servery, diskové polia sú v bezpečí**
- **Názov je odvodený z vojenského termínu „demilitarizovaná zóna“ ako oblasť medzi štátmi, mezi ktorými nie sú dovolené žiadne vojenské akcie**


Internet
External Firewall
DMZ LAN
DMZ System
Internal Firewall
Internal LAN
System 1
System 2
System n...

Firewall

- **Firewall je sieťové zariadenie a/alebo softvér na oddelenie sietí s rôznymi prístupovými právami (typicky napr. internet a intranet a kontrolovať tok dát medzi týmito sieťami**
- **Kontrola toku dát prebieha na základe aplikovania stanovených pravidiel a podmienok**
- **Podmienky sa stanovujú pre údaje, ktoré možno získať z dátového toku (napr. zdrojová, cieľová adresa, zdrojový alebo cieľový port a rôzne iné)**
- **Úlohou firewallu je vyhodnotiť podmienky a ak je podmienka splnená, vykoná sa jedna z 2 akcií "povoliť dátový tok" alebo "zamietnuť dátový tok"**
- **Obvykle sa používajú dva Firewally k vytvoreniu DMZ – jeden jako front-end len pre kontrolu DMZ a druhý jako back-end pre kontrolu toku dát medzi DMZ a vnútornou sieťou (intranet)**

SIEŤOVÁ BEZPEČNOSŤ

- **„Pravidlá správy a prevádzky lokálnej siete organizácie“, ktoré stanovujú najmä:**
- **Prístupové práva a identifikáciu používateľov**
- **Prideľovanie a správa domén druhej úrovne napr. @stuba.sk**
- **Pravidlá pre pripájanie zariadení do siete**
- **Pravidlá používania elektronickej pošty, vrátane prideľovania mailových adries**
- **Pravidlá prístupu k verejným webovým službám, vyhľadávačom a sociálnym sieťam**
- ***Organizácia má právo zakázať používanie prístupu na weby a sociálne siete z pracovných staníc zamestnancov***
- **Disciplinárny postih za porušenie „Pravidiel“**

SIEŤOVÁ BEZPEČNOSŤ

O problematike

- **adresovania a bezpečnosti internetu**
- **bezpečnosti aplikácie špecifických technológií**
- **bezpečnosti vo WIFI sieťach**
- **bezpečnosti cloudových služieb**

- ***Budeme hovoriť na nasledujúcej prednáške***

PREVÁDZKOVÁ BEZPEČNOSŤ

- **Zmluvy na dodávky HW a aplikačného SW alebo na ich údržbu musia obsahovať ustanovenia:**
  - **povinnosti dodávateľa zachovať mlčanlivosti**
  - **Sankcie za prípadnú haváriu systému spôsobenú preukázateľne vinou dodávateľa**
  - **Spôsob zachovania kontinuity systému v prípade vyhlásenia konkurzu resp. zrušenia činnosti dodávateľa**
- **Zabezpečovať priebežné kontroly dodržiavania bezpečnostných smerníc dátovej sieťovej, prevádzkovej a fyzickej bezpečnosti**

METÓDY A PROSTRIEDKY RIADENIA PROJEKTOV IS

- **Manažéri IT majú dve možnosti ako riadiť projekty implementácie IS**
- **Heroicky - riadiť projekty bez pevne stanovených pravidiel, iba na základe vlastného úsudku a skúseností - dôsledkom je**
- **nepredvídateľnosť výsledkov**
- **„únava materiálu" vypätie členov teamu vedie k fyzickému a psychickému vyčerpaniu**
- **objavovanie teplej vody - vývoj prostriedkov, ktoré existujú**
- **nedostatočná kontrola nad projektom, jeho zmenami**
- **z toho vyplývajúce neefektívne vynakladanie zdrojov peňazí a času**

- **použitie niektorého z medzinárodných štandardov**
- **tento prístup je istejší, vedie k predvídateľnejším výsledkom a lepšej kontrole nad projektom**
- **najvýznamnejšie medzinárodné štandardy projektového riadenia:**
- **Pôvodom britský štandard PRINCE2 dáva k dispozícii robustný a presný procesný model pokrývajúci predprojektovú prípravu, celý životný cyklus projektu**
- **definuje opisy rolí jednotlivých členov riadiaceho tímu a odporúčané obsahy riadiacich dokumentov**
- **neposkytuje podrobné techniky použiteľné pri riadení projektov a nepokrýva ani interpersonálne zručnosti potrebné pri projektovom manažmente**

- **PMI - Project Management Institute**
- **jeho základnou súčasťou je PMBOK Guide**
- **ide o súhrn množstva nástrojov a techník, ktoré môžeme využiť pri riadení projektov**
- **IPMA - International Project Management Association**
- **prináša do praxe ucelený hodnotiaci model odborníkov na projektové riadenie**
- **ide o podrobný zoznam spôsobilostí, ktoré má mať dobrý projektový manažér na príslušnej úrovni - od člena riadiaceho tímu projektu až po riaditeľa projektov**
  - **ako rýchlo a čo najobjektívnejšie posúdiť, či daný projektový manažér či člen riadiaceho tímu projektu má predpoklady zvládnuť svoju rolu v projekte**
  - **nezávislá certifikácia odborníkov na projektové riadenie**

- **RUP - Rational Unified Process - je metodika vývoja softvéru a určitého spôsobu riadenia projektu. Používa sa hlavne na veľkých IT projektoch, pre malé projekty je príliš zložitá**
- **SDLC - System Development Life Cycle – je proces vývoja lebo úpravy informačných systémov a modely a metodiky, ktoré sa používajú na ich vývoj. Koncepcia SDLC je základom mnohých ďalších metodík na vývoj softvéru.**
- **XP - Extreme Programming – je metodika vývoja softvéru usilujúca sa o zvýšenie kvality softvéru a zrýchlenie odozvy na meniace sa používateľské požiadavky. Podporuje časté odovzdávanie softvéru v krátkych časových intervaloch. Obsahuje mnoho podnetných myšlienok ako napr. programovanie vo dvojiciach, jednoduchosť a samodokumentovateľnosť kódu, neustále automatizované testovanie atď.**

- **SCRUM – je jednou z najrozšírenejších agilných metodík, vhodná pre s malými tímami, do 10 členov v tíme. Princípy: časté dodávky softvéru, postupné zlepšovanie, hľadanie najlepších stratégii fungovania tímu, intenzívna otvorená komunikácia atď.**
- **DSDM - Dynamic System Development Method – pôvodne metóda, ktorá mala vniesť určitú disciplínu do RAD , v súčasnosti je to univerzálny postup ako riadiť projekty a dodávky agilným spôsobom**
- **RAD - Rapid Applications Development– je metodika vývoja softvéru, z hľadiska riadenia minimalizuje plánovanie v prospech rýchleho zhotovenia prototypu. Je založená na myšlienke, že používateľské požiadavky sa najlepšie získavajú na prototype budúceho softvéru. Pri vývoji sa postupuje v iteráciách**

	PRINCE2	PMI PMBOK Guide	IPMA ICB
Procesný model	+	+	-
Definície rolí a zodpovedností	+	čiastočne	len projektový manažér
Nástroje a techniky	len 2	+	+
Osnovy / šablóny dokumentov	+	-	-
Interpersonálne a mäkké zručnosti	-	+	+
Akreditácia tréningových organizácií	+	len registrácia	-
Akreditácia trénerov	+	-	-
Akreditácia školiacich materiálov	+	len registrácia	-
Počet certifikovaných odborníkov celosvetovo	viac než 744.000	viac než 617.000	cca. 100.000
+ obsahuje - neobsahuje			

INFORMAČNÉ SYSTÉMY

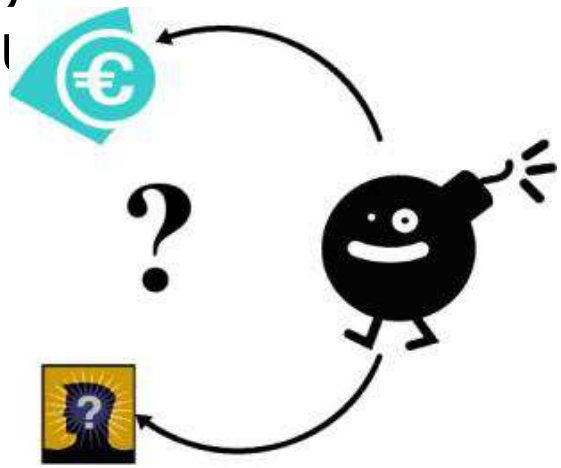
- **Životný cyklus procesu vývoja IS**
- **Univerzálny postup neexistuje, vždy to závisí od konkrétnych podmienok a cieľa vývoja IS**
- **Každý prístup má svoje plusy a mínusy**
- **Modelov pre realizáciu životného cyklu procesu vývoja IS je viac**
- **Naznámejšie sú model Big Bang, vodopád, špirálový model, inkrementálny a evolučný**

- **každý proces vývoja IS môžeme popísať prostredníctvím životného cyklu**
- **jeho základné etapy sú:**
- **požiadavky budúceho používateľa (investora) na IS**
- **tvorba konceptuálneho modelu záznam skutočností v rámci modelu, napr. obeh informácií v organizácii a kompetencie**
- **tvorba implementačného modelu - konkrétny návrh IS**
- **implementácia IS**
- **testovánie a uvedenie do skúšobnej prevádzky,**
- **prevádzka IS, vrátane údržby**
- **požiadavky na zmeny, zmenové konanie**
- **ukončenie používania systému**

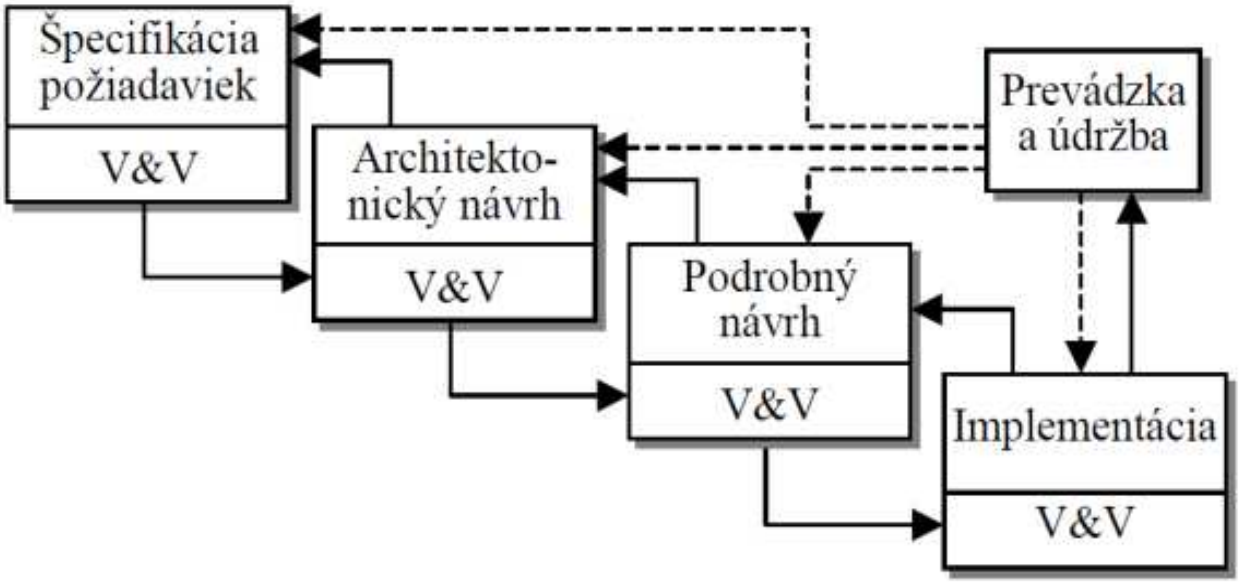
- **zber požiadaviek - interview**
- **špecifikácia požiadaviek je záväzná pre budúceho používateľa IS ako aj dodávateľa**
- **zmeny sú možné, ale vyžadujú schválenie od obidvoch strán a zohľadnenie všetkých vplyvov, rizík a prínosov**
- **cieľom špecifikácie je vytvorenie uceleného katalógu požiadaviek na funkcionality IS**
- **používatelia veľmi často nevedia formulovať svoje požiadavky na funkcionalily**
- **je potrebné vytvoriť priestor pre manažment dodatočných zmien špecifikácie**
- **čím presnejšia bude úvodná špecifikácia požiadaviek, tým jednoduchšie budú dalšie fázy vývoja IS**

- **ISO 12207**
- **norma ISO/IEC 12207 je mezinárodný štandard určený pre vývoj programových produktov v rámci životního cyklu (Software Life Cycle Processes)**
- **tento standard bol navrhnutý v r. 1988 a publikovaný v roku 1995 a je určený ako spoločný mezinárodný rámec pre vývoj, dodávky, podporu a údržbu programových produktov.**
- **štandard se zaoberá predovšetkým troma zásadnými procesmi**
  - **procesom primárneho životného cyklu**
  - **podpore procesov životního cyklu a**
  - **organizačným procesom životného cyklu**

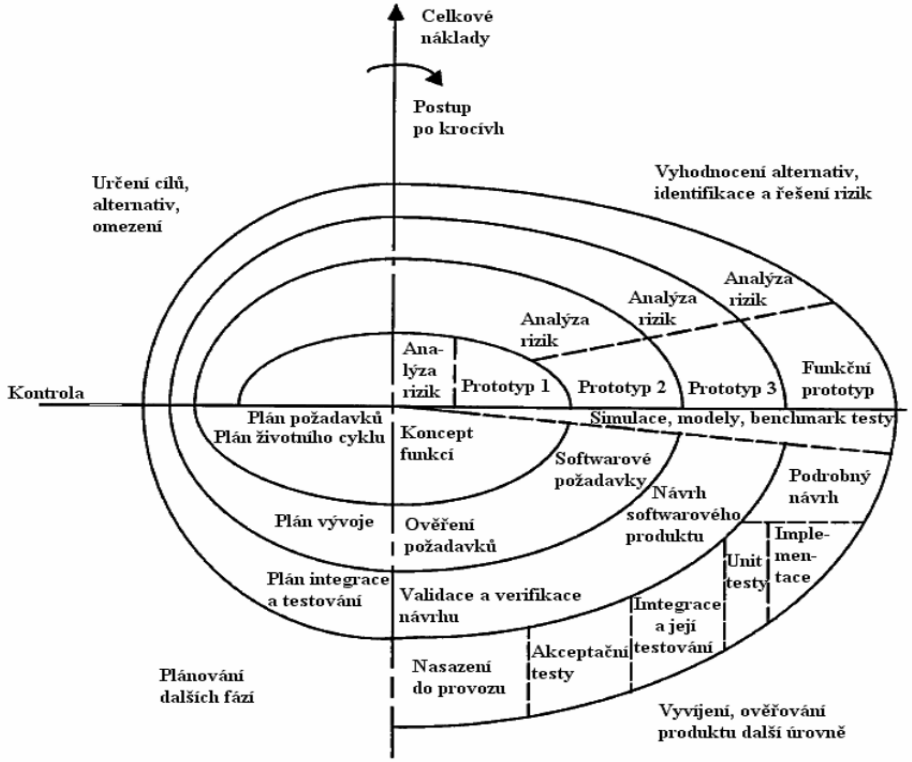
- **model Big Bang**
- **jednoduchá metóda , kde fázy špecifikácie a analýzy neexistujú, len sa programuje**
- **výsledok je že program funguje ako má alebo nefunguje**
- **testovanie spočíva v hľadaní chýb hotovej aplikácie.**
- **vhodný pre projekty, kde termín dodania výsledného produktu**



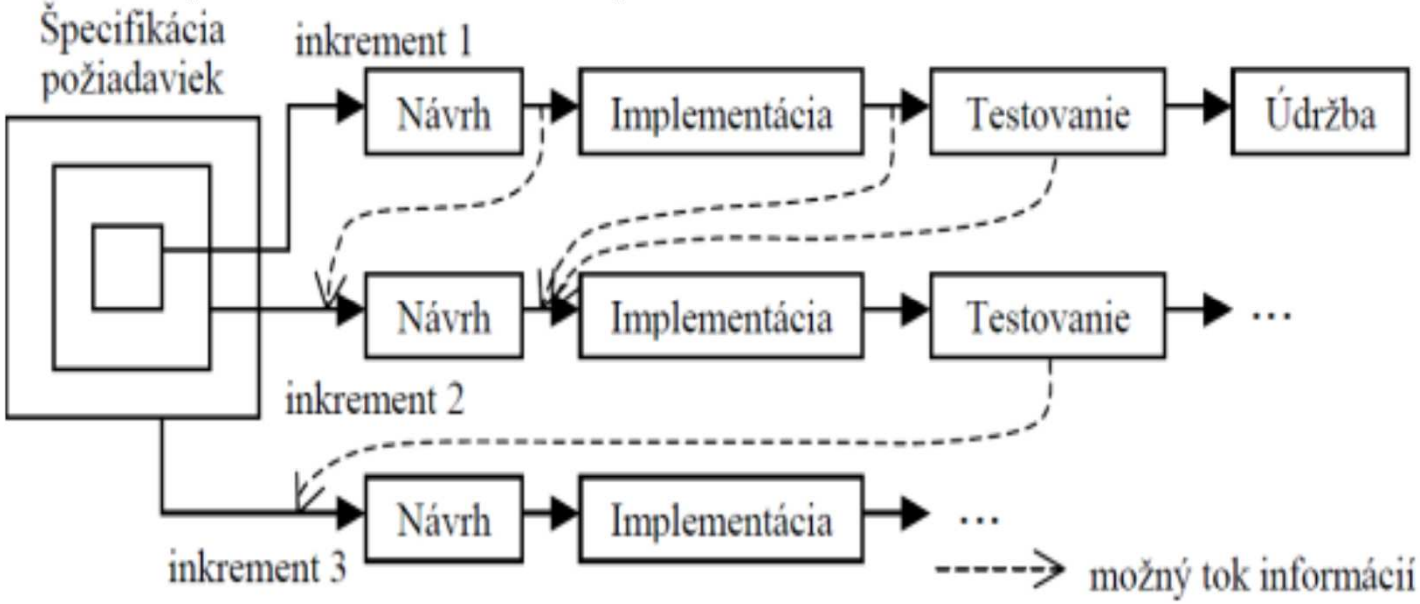
- **model „vodopád“**
- **jasne určená štruktúra, jednoduchý pre začínajúcich manažérov**
- **dôraz je kladený na fázu analýzy**
- **v zásade nie je možný návrat medzi fázami**
- **testovanie je až na konci cyklu**
- **pomerne statická štruktúra, nereaguje na zmeny.**



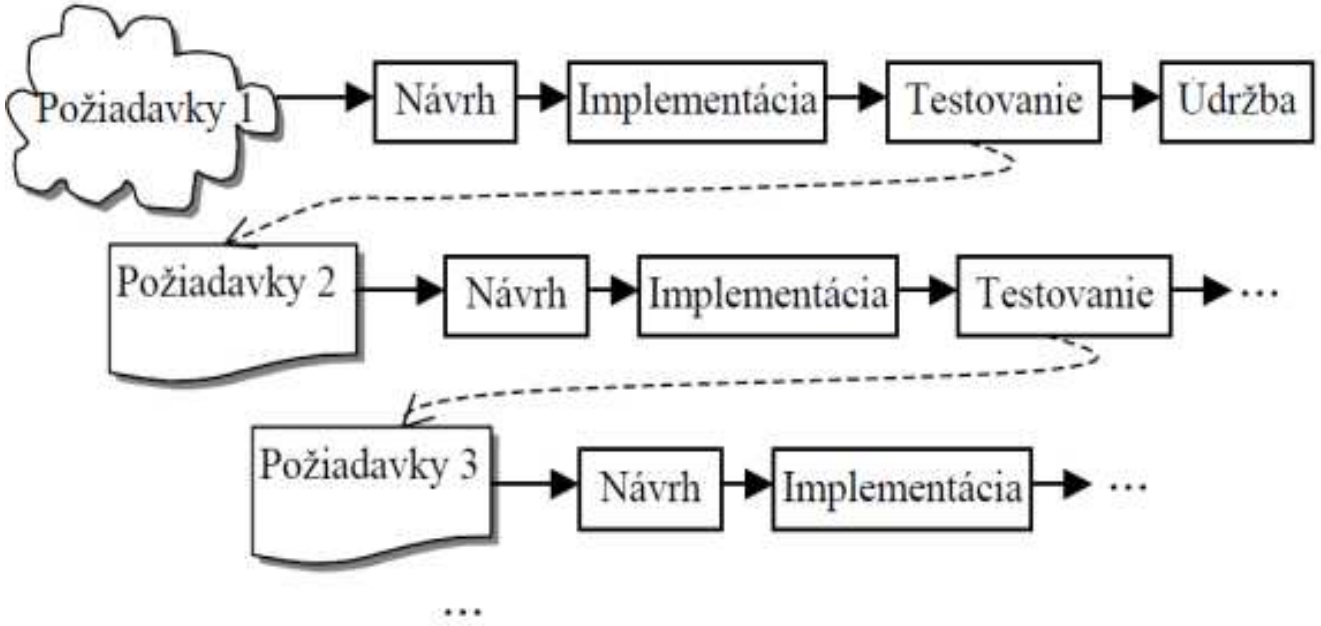
- **špirálový model sa dá rozdeliť do 4 hlavných častí**
- **určenie cieľov, alternatív, obmedzení**
- **vyhodnotenie alternatív, identifikácia a analýza rizík**
- **vývoj a verifikácia ďalšej úrovne produktu**
- **plánovanie nasledujúcích fáz riešenia**



- **inkrementálny model**
- **prírastkový, vychádza z katalógu požiadaviek na IS**
- **vytvára, prezentuje a odovzdáva IS použťívateľovi - investorovi po častiach**
- **vyžaduje úplnu a konzistentnú špecifikáciu požiadaviek používateľov kompletná**
- **ak takáto špecifikácia nie je vznikajú problémy v ďalšom pokračovaní procesu**



- **evolučný model**
- **začína spoločnou analýzou, nasleduje dekompozícia IS, pokračuje špirálovým modelom**
- **požiadavky sú špecifikované postupne v jednotlivých fázach**
- **používa sa v prípadoch, ak na začiatku procesu nevieme presne špecifikovať všetky požiadavky, napr. znalostné systémy**



- **Čo je a čo nie je IS verejnej správy**
- **predpokladom toho, aby určitý informačný systém mohol byť označený za ISVS, je predovšetkým naplnenie definičných znakov ISVS stanovených zákonom o ISVS verejnej správy – zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy v znení zmien a doplnkov**
- **k tomuto zákonu je ešte Výnos MF 55/2014 Z.z. z 4.3.2014 o štandardoch pre IS VS**
- **v zákone sú uvedené definičné znaky IS VS §2 zákona ako aj povinnosti povinných osôb, ktoré sú definované v §3 zákona (ÚOŠS ako aj ďalšie právnické osoby podľa ods. 3**
- **povinné osoby sú zodpovedné za vytváranie, správu a rozvoj IS VS**

- **Čo nie je kritériom pre určenie IS VS**
- **dostupnosť – rozhodujúce nie je, či je IS VS verejne dostupný alebo je neverejný**
- **outsourcing – kritériom nie je ani či IS VS prevádzkuje orgán verejnej správy alebo komerčný subjekt**
- **otázky na IS VS**
  - **bol by pri nefunkčnosti IS narušený alebo ohrozený výkon povinností vyplývajúci z kompetencií orgánu verejnej správy?**
  - **sú v IS uložené údaje o vykonávané správnej činnosti alebo údaje pre podporu výkonu u tejto činnosti?**
- **pokiaľ budú odpovede kladné ide o IS VS**
- **vždy však bude považovaný za ISVS taký informačný systém, ktorý je uvedený v zákone ako IS VS**

OUTSOURCING

- **Mýty a skutočnosť**
- **Kto má záujem na „predaji“ outsorcingu a kto má záujem na „kúpe“ outsourcingu**
- ***Pre komerčné firmy je niekedy jednoduchšie zamerať sa len na tzv. „core business“ a všetky ostatné činnosti odovzdať externým firmám, znamená to pre nich keď aj nie úsporu nákladov, ale aspoň nie veľkú stratu a firma sa môže sústrediť len na hlavnú činnosť’***
- **Kedy to nie je výhodné a v oblasti IKT to firmy ani nerobia**
- ***Keď by hrozilo bezpečnostné riziko vyzradenia citlivých údajov firmy***

OUTSOURCING cont.

- **Ako je to v vo verejnej správe**
- **Dá sa spočítať rozdiel medzi cenou na jednotku služby IKT vo VS formou interných útvarov a formou outsourcingu**
- ***Pre zabezpečenie bezpečnej a bezporuchovej prevádzky IPS je potrebný rovnaký počet úkonov pri obidvoch formách zabezpečenia***
- ***Interné útvary však majú nízku réžiu (energie, prenájom obslužné činnosti počítače), nepotrebujú vytvárať zisk***
- ***Naopak externá firma má tieto náklady oveľa vyššie (vyššie platy, prenájom vlastná réžia a pod.) a musí generovať zisk***
- ***Niekedy je však outsourcing nevyhnutný, pretože vysokosofistikované činnosti IKT špecialistov nie je možné zabazpečiť vo VS***

ÚLOHA IKT V ČINNOSTI ORGANIZÁCIE

- útvary IKT v organizácii v podmienkach ÚOŠS
- väčšina ÚOŠS v uplynulých rokoch zásadne redukovala počty zamestnancov a kvalifikačnú štruktúru útvarov IKT
- dôsledkom takéhoto vývoja je stav, kedy nie je splnená podmienka citovaného zákona o IS VS, že povinná osoba zodpovedá za vytváranie, správu, a rozvoj IS VS
- Ako to funguje teraz?
- ÚOŠS majú za úlohu inovovať IS VS alebo sa rozhodnú vytvoriť úplne nový napr. nový portál
- ÚOŠS jeho povinné osoby nedokážu vzhľadom na kapacitu a nízku kompetenciu zamestnancov vlastných útvarov IKT špecifikovať svoje predstavy a požiadavky

- **Akú sú možnosti?**
- **ÚOŠS zadá takúto úlohu externej „poradenskej“ firme**
- **„poradenská firma“ vykoná vlastne úlohy povinnej osoby v zmysle citovaného zákona a predloží špecifikáciu požiadaviek**
- **v ďalšom kroku sa vyberie firma, ktorá bude implementovať IS podľa dodaných požiadaviek a špecifikácie funkcionalít, ktoré si osvojil ÚOŠS**
- **ďalším problémom v tejto situácii je zostavenie riadiacej rady projektu vytváraného IS, pretože situácia bude nerovnovážna**
- **na strane dodávateľa dobre platení odborníci pre každú problematiku – štruktúra databázy, druh DBS, technické vybavenie, počty a výkon serverov, systémové prostredie, i.**
- **na druhej strane team ÚOŠS s podstatne nižšou kvalifikáciou**

- **Aké sú východiská**
- **1. doplniť a podstatne zlepšiť kvalifikačnú štruktúru útvarov IKT**
- **2. zabezpečiť permanentné školenia pre zamestnancov IKT , aby boli na zodpovedajúcej odbornej úrovni**
- **3. zvýšiť postavenie zamestnancov IKT a ich nadväzujúcich analytikov v štruktúre IKT, pretože títo zamestnanci sú zodpovední za rozvoj úrovne riadenia a efektivity výkonu verejnej správy**
- **príklady z komerčných firiem, kde je veľmi významná pozícia CIO - Chief Information Officer (CIO) or Information Technology (IT) Director, is a job commonly given to the most senior executive in an enterprise responsible for the information and computer systems that support enterprise goals**

Ďakujem Vám za pozornosť

OTÁZKY?