BEZPEČNOST IS

P1
2008-02-21

Čestmír Halbich

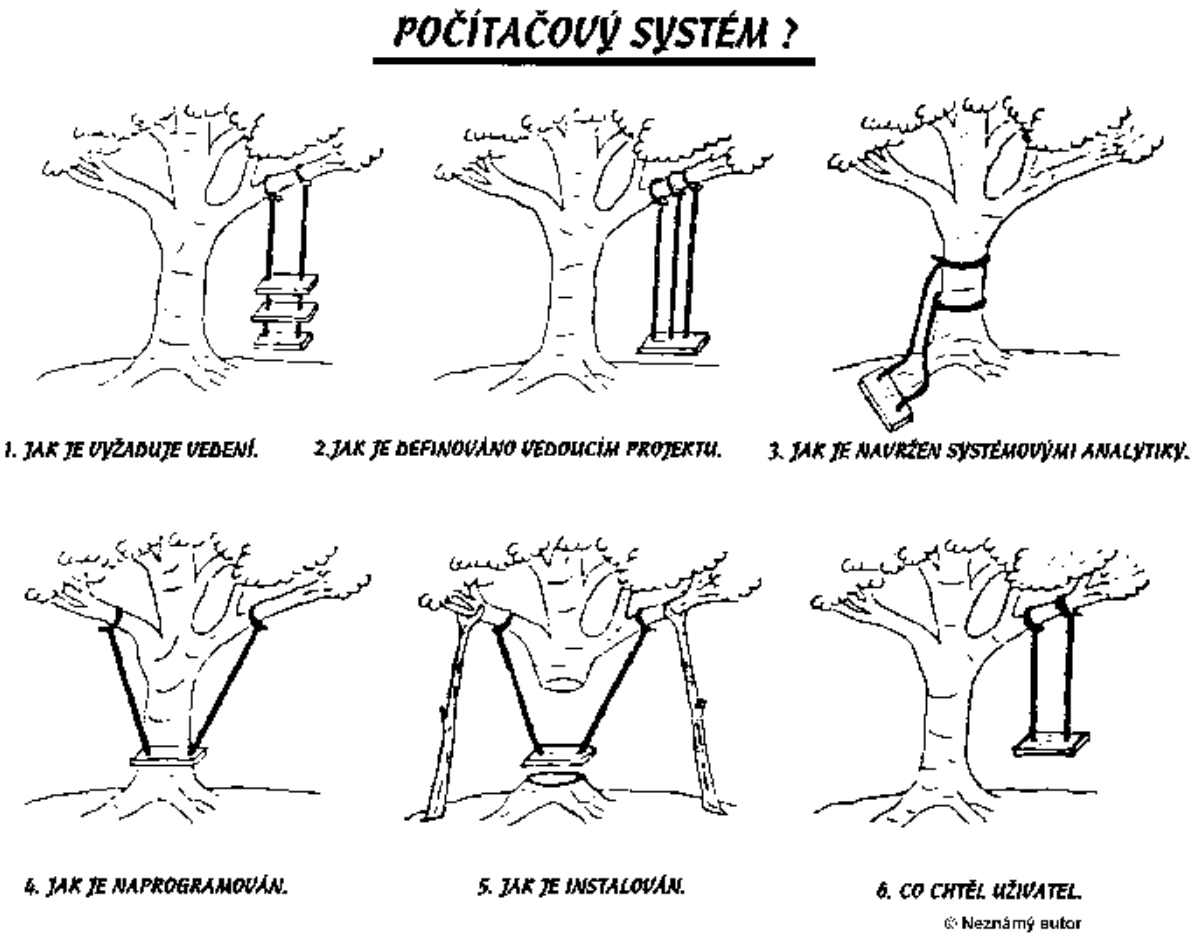
Skripta:
- ✓ Halbich, Brechlerová – Bezpečnost informačních systémů

Zkouška:
- ✓ Přes Moodle
- ✓ Ústní při nerozhodnutém výsledku nebo na vylepšení
- ✓ Zaškrtávací test a, b, c, d

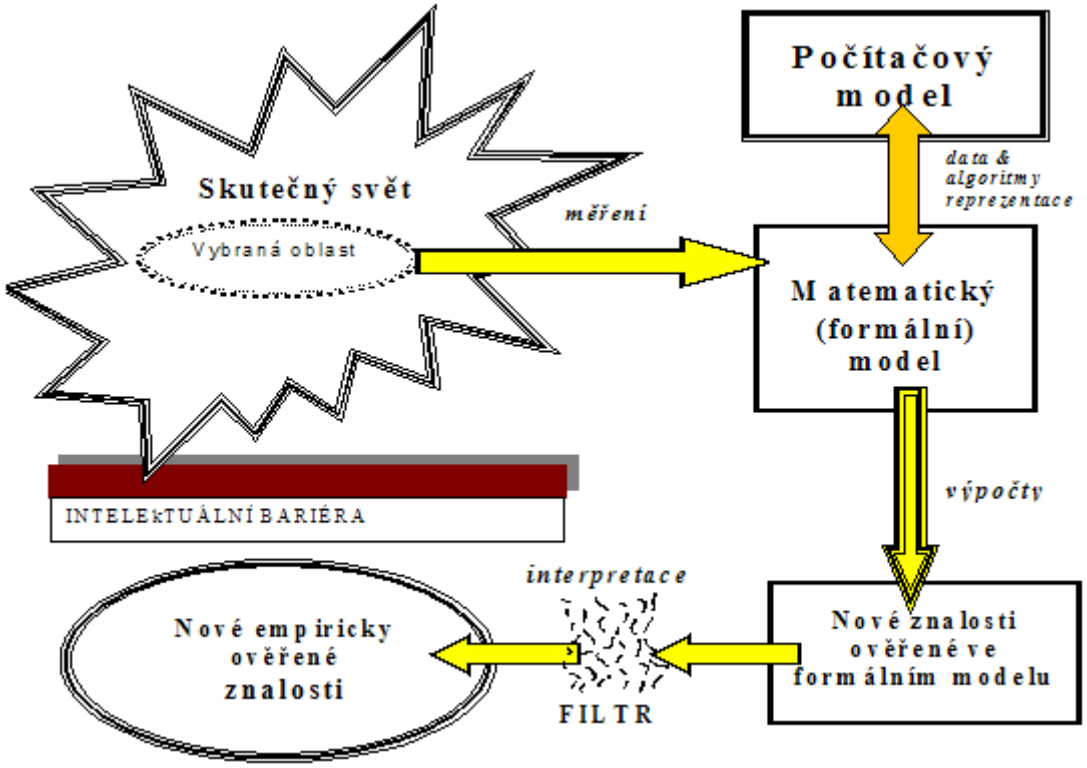
Cvičení:
- ✓ Cca společná práce
- ✓ Na zápočet nutno vypracovat projekt a na konci semestru prezentace projektů

Materiály:
- ✓ I:/KIT/halbich/bezp/2008/2008_01/predn21_2

SYSTÉM:

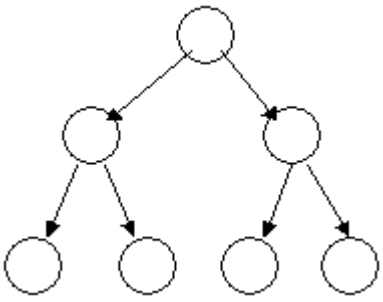


Použití principů formální matematické teorie a informačních technologií pro rozšíření lidských znalostí může být popsáno následujícím schématem:

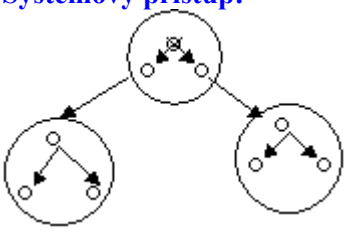


Systém a systémový přístup:

✓ **Definice systému:**

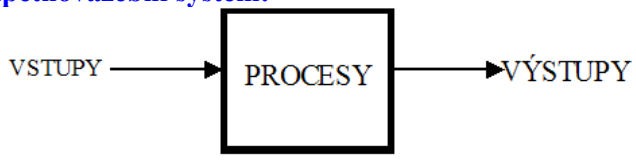


✓ **Systémový přístup:**

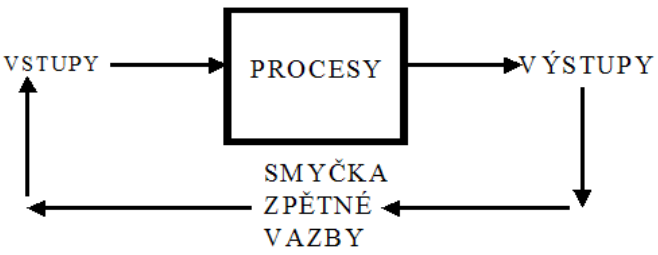


Typy systému:

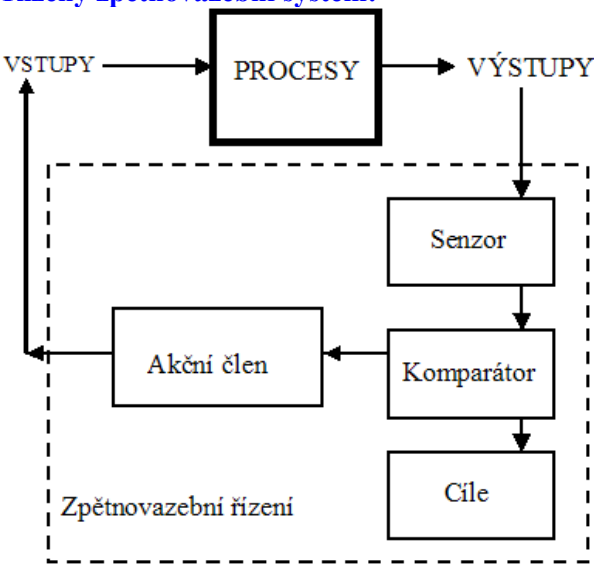
✓ **Zpětnovazební systém:**



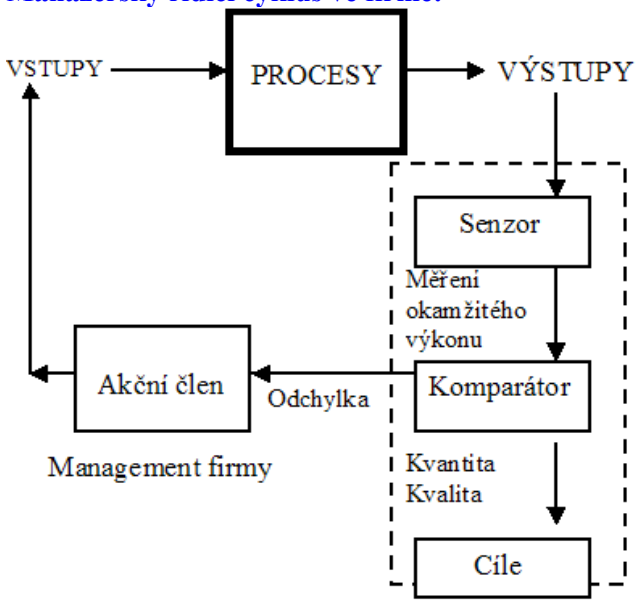
Jednoduchý model systému



✓ **Řízený zpětnovazební systém:**



✓ **Manažerský řídící cyklus ve firmě:**



Důvěryhodnost informace:
- ✓ Zastaralost informace
- ✓ Chybnost informací
- ✓ Nespolehlivost informací
- ✓ Informační přetížení
- ✓ Využitelnost informací
- ✓ Dostupnost informací

Informační soubor:
- ✓ Tvořen informačními soubory s jejich vzájemnými vztahy
- ✓ Klasické pojetí – množina informačních vět se stejnou logickou strukturou
- ✓ Objektové pojetí

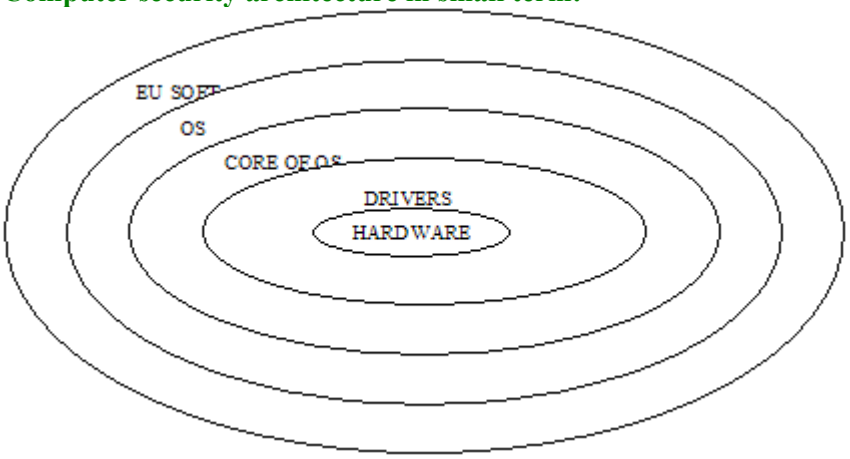
Informační systém:
- ✓ Informační systém je množina lidí, dat a postupů, které působí společně pro získání užitečných informací.
- ✓ Informační systém je nejen množina formálních informací, které cirkulují v podniku, ale jsou to též postupy a prostředky, které umožňují tyto informace definovat, vyhledávat, formalizovat, ukládat a distribuovat.

Models of security:
- ✓ Discretionary Access Control Model (DAC)
- ✓ Control of Information Flow
- ✓ Military Security Model
- ✓ Need-to-know Principle
- ✓ Bell and LaPadula Model
- ✓ Biba Model
- ✓ The Clark and Wilson Model
- ✓ THe Personal Knowledge Approach
- ✓ The Chinese Wall Policy

Computer architecture:
- ✓ The set of layers and protocols (including formats and standards that different hardware/software must comply with to achieve stated objectives) which define a computer system.
- ✓ Computer architecture features can be available to application programs and system programmers in several modes, including a protected mode. For example, the system-level features of computer architecture may

include: memory management, protection, multitasking, input/output, exceptions and multiprocessing, initialization, coprocessing and multiprocessing, debugging, and cache management.

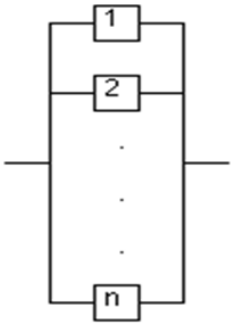
Computer security architecture in small term:



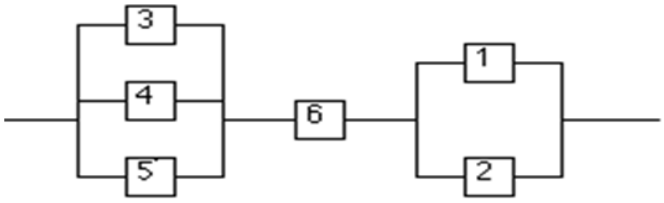
Examples:

- ✓ Series structures:

- ✓ Paralles structure:



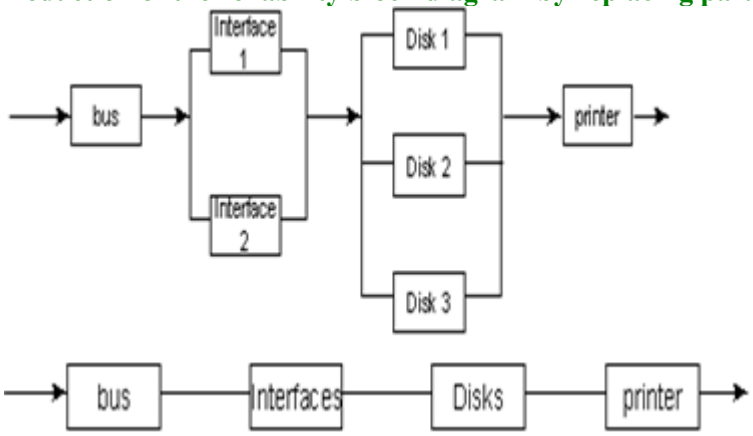
- ✓ Systém may also cosine both parallel and series structures:



Mean Time To Failure (MTTF):

- ✓ Expected time that a system will operate before the first failure occurs (first secure incident). The unreliability F(t) is $F(t)=1 - e^{-\lambda t}$ and reliability R(t) $R(t) = e^{-\lambda t}$.
- ✓ MTTF = $1/\lambda$
- ✓ For $\lambda t << 0,1$ we have a good approximations: $R = 1 - \lambda t$ and $F = 1 - \lambda t$
- ✓ Risk assessment of the system which consists from n elements with risk of failure $\lambda_1, \lambda_{2, \ldots} \lambda_n$
- ✓ Is computed from the formula $R_c = R_1 \ . \ R_2 \ . \ Rn \ = \ e^{-\lambda_1 t} \ . \ e^{-\lambda_2 t} \ \ldots . \ e^{-\lambda_n t} \ = e^{-\lambda_c t}$
- ✓ The finite risk failure value is the sum of risk failure values of the individual components in the case of the reliability of series systems, assuming l_i are independent
  $R_1(t) = R_2(t) = R_3(t) = 0.9$
  $R_{series}(t) = 0.9 \ . \ 0.9 \ . \ 0.9 = 0.729$

Reduction of the reliability block diagram by replacing parallel portions with an equivalent single element:



Informační systém:

- ✓ IS nemusí být nutně veden na počítači. Z hlediska právních předpisů není situace v oblasti vedení IS, forem evidencí, seznamů, či např. účetních knih jednoznačná (závisí na vůli provozovatele?). Podle Smejkala v našem právním řádu existuje v současné době 1087 platných právních předpisů, kde se vyskytuje slovo DOKLAD, 806 platných právních předpisů, kde se vyskytuje slovo DOKUMENT a 335 platných právních předpisů, kde se vyskytuje slovo PODPIS. Zákon ani jednoznačně nezakazuje či připouští vést dokumentace a evidence v určité formě, a to ani v novější formě elektronické. Existují výjimečně i právní předpisy, které vylučují elektronickou formu IS (např. zák. č. 36/1967 Sb. a prováděcí vyhláška o znalcích a tlumočnících, kteří musí vést deník. Ten je složen z pevně spojených průběžně číslovaných listů a opatřen pečetí krajského soudu. Běžná elektronická podoba by těžko splňovala tyto náležitosti.)
- ✓ **Bezpečný informační systém** zajišťuje:
  - **Důvěrnost** – tj. přístup k informacím mají pouze autorizovaní uživatelé
    Pozn.: Autorizace je definována jako určení, zda subjekt (uživatel nebo systém) je důvěryhodný z hlediska jisté činnosti, např. čtení daného souboru.) uživatelé.
  - **Integritu** (neporušitelnost - tj. modifikovat data mohou pouze autorizovaní uživatelé)
  - **Dostupnost** služeb poskytovaných autorizovaným uživatelům systémem
  - Řada **podpůrných služeb**, funkcí podporujících bezpečnost, jakou je např. účtovatelnost všech důležitých akcí, aby bylo možno prokázat přístup jednotlivých subjektů ke konkrétním informacím a zdrojům informačního systému, tj. k jeho objektům.

Bezpečnostní politika:

- ✓ **Bezpečnostní politika** specifikuje míru závažnosti a obsah té které složky bezpečnosti pro konkrétní informační systém. Bezpečnostní politika systému pracujícího pro ministerstvo vnitra bude zřejmě klást největší důraz na důvěrnost, naproti tomu bezpečnostní politika systému komerční firmy na integritu, bezpečnostní politika systému telefonní společnosti na dostupnost.
- ✓ Bezpečnostní politika má obvykle charakter **povinných zásad**, měnitelných pouze několika správci. Na bezpečnostní politiku můžeme pohlížet jako na normy, pravidla a praktiky definující způsob zpracování, ochrany a distribuce citlivé informace v rámci činnosti AIS.
- ✓ Autorizaci předchází **autentizace**, tj. proces, kterým se poskytuje záruka týkající se identity subjektu nebo objektu, např. ujištění, že konkrétní uživatel je skutečně ten, za kterého se prohlašuje, resp. schopnost zjistit, kdo vydal daný příkaz nebo požadavek. Např. nejjednodušší je autentizace heslem, avšak je nejsnáze napadnutelná (zvláště v ETHERNETových sítích).
- ✓ AIS, který svojí realizací splňuje bezpečnostní politiku, nazýváme **důvěryhodný systém**. Důležitou podmínkou bezpečnosti AIS je zájem uživatelů na jeho bezpečnosti. Standardy bezpečnosti AIS mají se souvisejícími normami tisíce stran textu, pokud je slabina AIS v oblasti lidského činitele (ať již u uživatelů, nebo správců apod.), nezabrání ani bezpečnostní politika úniku dat. Tyto standardy jsou však důležité, protože existují různá další rizika porušení bezpečnostní politiky. Proto se bezpečný systém nevyhne ani používání takových služeb a funkcí, jako jsou audit.

- ✓ **Audit** znamená, že se zaznamenávají všechny signifikantní události pro bezpečnost AIS, ke kterým dojde při jeho činnosti a záznamový mechanismus by neměl být "uplatitelný"". Auditní služby jsou obvykle úzce svázány s autentizačními a autorizačními službami. Zaznamenává se každý pokus o zpřístupnění objektu bez ohledu na to, zda se jednalo o autorizovaný přístup. Auditní záznam lze použít pro účtování činností jednotlivých subjektů, ale také pro analýzu chování jednotlivých uživatelů, maškarád (tj. narušitel se vydává za někoho jiného, obvykle autorizovaného), apod., procedury pro detekci poruch, procedury pro obnovu po poruše apod.
- ✓ Z filosofického hlediska a z hlediska teorie systémů lze usoudit, že neexistuje žádná bezpečnostní politika, která by zaručila absolutní bezpečnost AIS. Absolutní bezpečnost AIS lze dosáhnout pouze jeho absolutní izolovaností, tzn. vyloučením všech vstupů resp. výstupů do/ze systému- žádné praktickému využití. Zvolený rozsah bezpečnosti efektivně pracujícího systému je proto vždy kompromisem mezi cenou, kterou jsme ochotni za bezpečný systém zaplatit a mírou rizika, kterou jsme ochotni připustit.(Pozn. tato cena je obvykle vyšší než cena samotného hardware.)
- ✓ Je třeba zvážit hodnotu zabezpečovaných aktiv AIS, **zranitelnost** systému, **hrozby**, **rizika**, ceny možných poruch a jejich obnovy, stanovisko organizace k rizikům apod. Dále je třeba uvážit dostupná **protiopatření**, jejich efektivnost, cenu jejich instalace a jejich provozní náklady.
- ✓ AIS jsou zranitelné zejména z následujících důvodů:
  - Vysoká hustota uložených a zpracovávaných informací
  - Složitost použitého software
  - Existence skrytých vazeb a kanálů při zpracování informací
  - Elektromagnetické vyzařování spojené s činností technických prostředků AIS

Oblasti opatření v ochraně dat:

- ✓ **Fyzická bezpečnost** např. fyzická ochrana a organizace fyzického přístupu ke zdrojům organizace, umístění monitorovacích zařízení, stanovení odpovědností a hierarchií, (v organizacích si děti uklízeček pouští na počítači hry z donesené diskety …-)
- ✓ **Personální bezpečnost** např. profesní a osobní kádrování, způsob uzavírání pracovních dohod, výpovědí, způsob profesní výchovy a dalšího vzdělávání,
- ✓ **Komunikační bezpečnost** např. bezpečnost komunikačních přenosů, spojů, použití šifrování, modemů, komutovaných linek, ochrana proti odposlechu,
- ✓ **Administrativní bezpečnost** a administrativa bezpečnosti např. vstupní a výstupní kontroly, postupy při certifikaci a akreditaci, podávání zpráv o incidentech (narušení bezpečnostní politiky), řízení změn konfigurací AIS, vedení dokumentace,
- ✓ **Analýza rizik** tj. vyhodnocení zranitelnosti a hrozeb zdrojů IS a plánování odpovídajících protiopatření,
- ✓ **Plánování postupu po incidentu**, který způsobí porušení bezpečnosti, přičemž mezi typické incidenty patří např. poškození, porucha, zničení požárem apod.
- ✓ **Účel bezpečnostní politiky** – bezpečnostní politika musí definovat strukturu správy programového systému, zodpovědnosti jednotlivců i skupin, resp. týmů v organizaci a celkové bezpečnostní cíle. Důležitou roli zde hraje zdůraznění úlohy jednotlivce a osobní zodpovědnosti každého zaměstnance organizace zavádějící bezpečná AIS (proto je žádoucí zavést detailní účtování činností jednotlivců).
- ✓ **Bezpečnostní politika** by měla pokrýt všechny zdroje IS v organizaci (hardware, software, informace, personál atd.). Jsou-li některé kritičtější, mělo by to být jednoznačně stanoveno