Vysokoškolská skripta

VŠE

FAKULTA INFORMATIKY A STATISTIKY

REPETITORIUM PRO INFORMAČNÍ MANAGEMENT

MATERIÁLY PRO PŘÍPRAVU K PŘIJÍMACÍMU ŘÍZENÍ NA NAVAZUJÍCÍ MAGISTERSKÝ STUDIJNÍ PROGRAM INFORMAČNÍ MANAGEMENT

PhDr. Ing. Antonín Pavlíček, Ph.D.

Ing. Richard Novák, Ph.D.

Ing. Luboš Pavlíček

PhDr. Věra Radváková, Ph.D.

Mgr. Jana Syrovátková

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky
Katedra systémové analýzy

Repetitorium pro Informační management

Materiály pro přípravu k přijímacímu řízení na navazující magisterský studijní program Informační management

Antonín Pavlíček
Richard Novák
Luboš Pavlíček
Věra Radváková
Jana Syrovátková

Praha
2022

Recenzentka: Ing. Lucie Böhmová, Ph.D.

Zdroj všech schémat a tabulek uvedených v této publikaci je vlastní práce autorů.

ISBN 978-80-245-2447-4

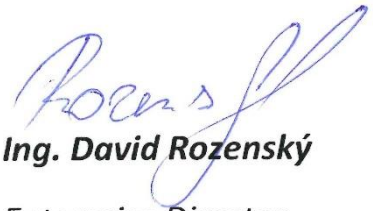
Úvodní slovo manažera z praxe

Byznys požadavky na absolventy vysokých škol se velmi rychle proměňují v čase a hodně se liší oborová poptávka na konkrétní specializace. Co však podle mě je zásadní a neměnné, je schopnost vidět věci v kontextu, mít celkový přehled o IT a schopnost se rychle učit.

Za svůj profesní život jsem již zažil obrácený důraz buď na izolovaná a bezpečná datová centra, ohraničené clustery IT, anebo teď naopak „hype" migrovat vše do vzdálených SaaS, PaaS, IaaS cloudů. Obojí má řadu příznivců i odpůrců, kteří se mění v čase. Co však zůstává shodné, je důraz na systémovou práci s informacemi, znalost byznysových a technických procesních vazeb, a také důraz na informační bezpečnost a odolnou IT architekturu. Poznat, navrhnout a posoudit dobré IT řešení, které naplní sledované technické i finanční metriky, vyžaduje dnes více systémové myšlení než znát nazpaměť jednotlivé bity a byty.

Myslím, že na Katedře systémové analýzy (KSA FIS) se učí ten správný mix informatických znalostí s důrazem na IT Governance, IT Bezpečnost a kombinované rozhodování manažerů i strojů. Tento moderní přístup k Informačnímu managementu připraví podle mne studenty velmi dobře na jejich budoucí uplatnění v praxi.

Studium na Katedře systémové analýzy (KSA) v rámci Fakulty informatiky a statistiky mohu tedy z pohledu mé vlastní zkušenosti studentům doporučit.



Ing. David Rozenský

Enterprise Director

T-Mobile Czech Republic

Obsah

VŠE / FAKULTA INFORMATIKY A STATISTIKY

Úvod do Informatiky
Repetitorium pro přijímací zkoušky

Antonín Pavlíček
Jana Syrovátková

Vysoká škola ekonomická v Praze

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

Data, informace

Vysoká škola ekonomická v Praze

Poznámky:

.....

.....

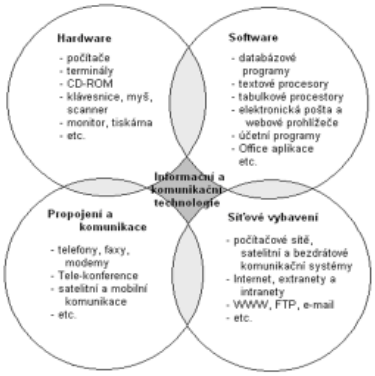
.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

ICT / informatika / informační věda



- ICT – zkratka informační a *komunikační* technologie
- Informatika

  sběr, zpracování, zobrazení, vyhledávání, řízení, uchovávání, využívání a kontrola dat a informací pomocí počítačů
- Informační věda

  knihovnictví, kybernetika, informace jako jev v lidském vědomí

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Informace – různé definice

- Je čerpání zpráv nebo obsahu z vnějšího světa *(N. Wiener, 1948)*
- Je vlastnost odstraňující apriorní neznalost příjemce *(C. E. Shannon, 1949)*
- Je význam přisuzovaný datům *(ČSN 36 9001)*

INFORMACE je zpráva o tom, že nastal určitý jev z množiny možných jevů a tím se u příjemce snižuje nebo zcela odstraňuje neznalost o tomto jevu.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Data a informace

Data – reprezentace skutečnosti

- Skutečnost, respektive její charakteristiku reprezentuje / zastupuje
- Sama o sobě bez významu
- Datům jednotlivec přisuzuje v procesu interpretace na základě své individuální znalosti určitý význam

Informace je pak právě tento význam přisouzený datům

- Každý jednotlivec interpretuje skutečnost ve své mysli. Interpretace dat je **individuální** a zároveň podléhá přijatým znalostem ostatních jedinců. Člověk je schopen přijmout určitou interpretaci dat, i když ji osobně nezkusil (neprožil)

Hodnota dat – potenciál jejich budoucí přeměny na srozumitelné informace

Poznámky:

.....

.....

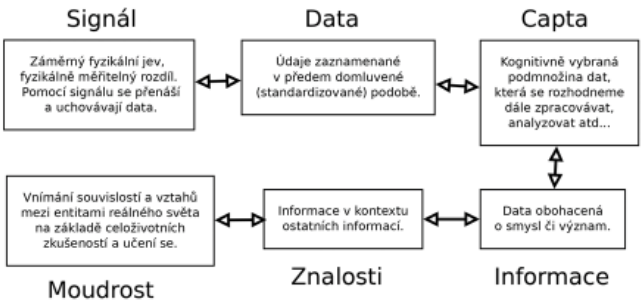
.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Signál -> Data (Capta) -> Informace -> Znalosti



Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Míra informace a entropie

- Základním pojmem v teorii informace je entropie (neuspořádanost, neurčitost). Znamená míru neurčitosti ve zprávě. Informaci pak chápeme jako odstranění této neurčitosti. S narůstající informací klesá entropie a naopak.
- C. E. Shannon definuje entropii: *„Předpokládáme existenci nějakého systému a současně předpokládáme samostatnou událost (nezávislou na předchozích událostech), která způsobí přechod systému do nového stavu. Předpokládejme n vzájemně se vylučujících stavů s_i, pravděpodobnost stavu i je $P(s_i)$, pak entropie stavu S bude:*

$$H(S) = -\sum_{i=1}^{n} P(s_i) log_2 P(s_i).\text{"}$$

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Míra informace - vysvětlení

Pro technické vyjádření míry informace se používá měření vycházející z teorie informace a je matematicky formalizováno na základě pravděpodobnosti výskytu:

- Existuje množina jevů s různou pravděpodobností výskytu.
- Pokud nastane jev, který „hodně“ očekáváme (pravděpodobnost 0 nebo 1) – míra informace o tomto jevu bude nízká.
- Nastane-li jev, který jsme „méně“ očekávali (pravděpodobnost blízká 0,5) – míra informace o tomto jevu bude vysoká.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Kvalita informace

Obtížně kvantifikovatelná, ale existují některá kritéria, např.:

- Spolehlivost – do jaké míry informace odpovídá realitě, ze které byla identifikována.
- Důvěryhodnost – zabezpečení proti manipulacím jakéhokoliv (lidského, technického,…) charakteru.
- Solidnost – korektní informace v rámci kontextu.
- Aktuálnost – stará zpráva o počasí pravdivá, ale zpravidla neužitečná.
- a existují další kritéria – např. úplnost, dostupnost, …

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Kvalita a rozsah

- Kvalita a rozsah informací se odvíjí od způsobu, kterým se o informaci dovídáme. Vliv na kvalitu informace má i věrohodnost zdroje – poskytovatele informace.
  - **Informace o informaci** (odkaz na jiný zdroj informace)
    - Největší prostor pro využití informační technologie – vyhledávání v informačních systémech (citace)
  - **Informace částečná**
    - Např. Popis trasy zájezdu podávaný průvodcem,
  - **Informace úplná**
    - Např. Podrobný výklad místního průvodce o historii a expozici daného zámku, monografie o dané lokalitě, CD-ROM obsahující věrnou kopii originální produkce atd.

10

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Kódování vs. šifrování

- Informace v počítači – jedničky a nuly
- Jiné znaky – zakódované pomocí 0 a 1
- Smysl kódování
  - Standardizovat a zjednodušit přenos/uložení informace
  - Zmenšit velikost / zvýšit rychlost přenosu
  - Zabránit chybám při přenosu
- Smysl šifrování
  - Ukrýt přenášenou informaci
  - Nahrazení znaků kódy bez klíče je šifra, ale smysl je jiný

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Databázový systém

- Nástroj pro uchování dat a pro tvorbu databázových aplikací
- Organizovaný soubor dat a nástrojů pro práci s daty uloženými na paměťovém médiu

Relační databázové systémy

- Data v provázaných tabulkách

např. tabulka studentů, jiná tabulka zapsaných předmětů, jiná tabulka pro známky, při změně příjmení sňatkem měním pouze tabulku studentů

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Objektově orientovaný relační databázový systém

- Informace formou objektů
- Každý objekt má vlastnosti a přípustné hodnoty, funkce u objektů, reakce na chování ostatních
- *Příklad – políčko v tabulce, smí tam být pouze číslo, je popsáno, co se stane, pokud se uživatel pokusí přepsat (např. přepočítání kreditů po zápisu známky z předmětu)*

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Databázové aplikace - obsah

- Data
- Datové struktury (vztahy mezi daty)
- Informace o přístupových právech
- Systém řízení báze dat
  - Komponenty (programy) pro správu
    - dat
    - uživatelských práv

Typicky různá počítačová rozhraní, nyní často webová, umožňující vkládat nová data, nastavovat práva, prohlížet data a další.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Data v databázové aplikaci

- **Primární data**
  - Základní smysl celé aplikace
  - Jména, adresy, telefonní čísla…
- **Metadata**
  - Informace o primárních datech
    - Vztahy mezi nimi
    - Přístupová práva k různým datům
    - Data napomáhající práci s daty
  - Informace o typu dat (délka jména, tvar telefonního čísla), studijní oddělení může přepisovat jména studentů, pedagog pouze prohlížet
- **Index**
  - Předpřipravený seznam (např. Podle abecedy) – pro rychlejší vyhledávání

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Informační systém - definice

INFORMAČNÍ SYSTÉM je
souhrn **lidí** & **ICT** & **dat** & **metod** (programů)
ZABEZPEČUJÍCÍ
sběr – **přenos** – **zpracování** – **uchování** dat
S CÍLEM
tvorby & **presentace** & **distribuce** informací
PRO
koncové **uživatele** informačních systémů.

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

HARDWARE

Vysoká škola ekonomická v Praze

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Kódování v počítačích

- Počítače se vyvinuly z mechanických (ozubené kolo), přes elektro-mechanických na čistě elektronické
- Všechny elektronické ale založeny **na principu proměnlivé elektrické vodivosti** – z praktického hlediska se ujala binární reprezentace – stavy 1 a 0/ true-false / proud teče – neteče
- Základní jednotkou informace je Binary digIT (BIT)

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Proč je výhodná dvojková soustava

- Existovaly sice počítače, které byly TRINARY či dokonce QUINARY – ale byl problém určit přesný stav elektrického proudu (Volty) /slabá baterie či rušení snížilo napětí - dvoustavové měření má největší vzdálenost stavů /třeba 0-1 V je stále nula, 3-5 V je jednička)
- Navíc - Pro binární stavy existuje ucelená oblast matematiky – Boolovská algebra (známá pravidla, operace, …)

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

„Spínače“ jednotlivých počítačových generací

- **Nultá generace** – elektromagnetická relé
- **První generace** (1945 až 1950) – elektronka
- **Druhá generace** (1951 až 1964) – tranzistor
- **Třetí generace** (1965 až 1980) – integrovaný obvod
- **Čtvrtá generace** (od roku 1981) – mikroprocesor

- Budoucnost – kvantová???

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Jak počítače počítají?

- Všechny elektronické ale založeny na principu proměnlivé elektrické vodivosti – z praktického hlediska se ujala binární reprezentace – stavy 1 a 0/ true-false / proud teče – neteče
- Pro binární stavy existuje ucelená oblast matematiky – Boolovská algebra (známá pravidla, operace, …)

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Umí počítač počítat?

5 + 10 = 15 – jak sečíst binárně?

16 8 4 2 1 - převodník do binára

1 0 1 (dekadicky 5)
1 0 1 0 (dekadicky 10)
======= Logický XOR
1 1 1 1 (dekadicky 15)

22

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Hardware osobního počítače

- Veškeré fyzicky existující technické vybavení
- Dnes typicky základní deska, procesor, paměť, pevný disk, zdroj a další

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Základní deska

- Společná základní deska (mainboard, motherboard) celého počítače
- Obsahuje napájecí obvody, konektory pro připojení procesoru, paměti a periferií (vnějších i vnitřních)
- Obsahuje řadiče sběrnic a obvody pro boot počítače po zapnutí (BIOS)
- Dnes často obsahuje i četné integrované periferie

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Procesor

- Hlavní výpočetní část počítače
- Vykonává strojový kód uložený v paměti počítače
- Soudobé procesory obsahují více paralelních (víceméně samostatných) jednotek označovaných jako jádra

Poznámky:

.....

.....

.....

.....

Paměť

- Místo, kam je možné ukládat data a programový kód (instrukce)
- Paměť označována jako RAM dle způsobu přístupu k uloženému obsahu (random access memory)
- Po vypnutí napájení se uložený obsah ztrácí

Poznámky:

.....

.....

.....

.....

Grafická karta

fis.vse.cz fisvse

- Zajišťuje zobrazení obrazu na monitoru
- Kancelářské počítače mívají integrovanou grafickou kartu (levná, nízká spotřeba)
- Pro hry a video je potřeba velkého výpočetního výkonu – externí grafické karty

Poznámky:

.....

.....

.....

.....

Pevný disk (HDD)

fis.vse.cz fisvse

- Klasické řešení označované jako HDD obsahuje mechanické disky (plotny) z magneticky měkkého materiálu, které jsou neohebné (pevné)
- Čtení i zápis jsou realizovány pomocí elektromagnetické indukce
- Data jsou organizována do stop rozdělených na jednotlivé sektory, pro rychlost čtení a zápisu (výkon disku) je podstatná rychlost otáčení ploten a celková architektura disku, řadič disku apod.
- Disky vykazují poměrně velkou spotřebu el. Energie

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Solid-state disk (SSD)

- SSD technologie odpovídá flash pamětem
- Disk neobsahuje mechanické části
- Výhodou je velká rychlost čtení, nevýhodou je poměrně nízká životnost média, resp. Jednotlivých datových buněk
- Spotřeba SSD disku je nízká, disk je nehlučný, mechanicky odolný, nevadí mu otřesy

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Hybridní disky (SSHD)

- Kombinace klasického mechanického HDD s SSD, typicky např. 1 tb hdd + 64 gb ssd
- Teoreticky poskytuje z každé technologie to lepší, tedy vysokou rychlost čtení SSD a zároveň velkou kapacitu HDD úložiště
- Řadič disku vybírá úložiště pro data tak, aby často používaná data byla uložena v SSD části disku

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Rozhraní počítačů

- Slouží ke komunikaci PC s okolím, typicky s periferiemi jako jsou monitory, tiskárny, přenosné disky, různá elektronická zařízení apod. (Vnější rozhraní), nebo ke komunikaci jednotlivých částí PC jako jsou procesor, paměti, grafická karta apod. (Vnitřní rozhraní)
- Jsou charakterizována
  - Hardwarovým uspořádáním (použité konektory, zapojení vodičů)
  - A použitým komunikačním protokolem (definicí způsobu komunikace mezi PC a periferií)

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Vnitřní rozhraní počítačů

- Rozhraní pro připojení vnitřních zařízení počítačů (paměť, pevné disky, rozšiřující karty, …)
  - Rozhraní pro pevné disky (SATA)
  - Rozhraní pro rozšiřující karty (PCI, PCI express)
  - Napájecí konektory
  - Rozhraní pro paměti, procesor, …

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Vnější rozhraní počítačů

- rozhraní pro připojení vnějších zařízení – např. audio a video
  - VGA, DVI, HDMI

Poznámky:

.....

.....

.....

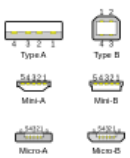
.....

fis.vse.cz fisvse

Vnější rozhraní počítačů - USB (Universal Serial Bus)

- USB 1.1
  - Low-Speed 1,5 Mbps
  - Full-Speed 12 Mbps
- USB 2.0 (2000)
  - Hi-Speed 480 Mbps
- USB 3.1 (2010)
  - Super-Speed 5 Gbps, gen II 10 Gbps
- USB C
  - 10 Gbps, oboustranný konektor
- USB 4.0 (2019)
  - 40 Gbps

- Limitovaný odběr ze sběrnice, resp. Napájení
- Zpětná kompatibilita
- Jednoznačná identifikace zařízení



Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Vnější rozhraní počítačů

- Rozhraní pro počítačovou síť
  - Konektor RJ45

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Bezdrátová komunikace

- Bluetooth
  - Nejtypičtěji pro párování dvou zařízení (bezdrátová myš, přenos dat mezi mobilními telefony…)
  - V bezlicenčním pásmu 2,4 ghz
- Wifi sítě
  - Nejtypičtěji pro připojování k internetu
  - V bezlicenčních pásmech 2,4 ghz a 5 ghz

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Periferie pro přímou komunikaci s uživatelem

VSTUPNÍ

- Počítačová klávesnice
- Počítačová myš
- Trackball
- Trackpoint
- Tablet
- Joystick
- Gamepad
- Scanner
- Webová kamera

VÝSTUPNÍ

- Monitor
- Reproduktor
- Tiskárna
- 3D tiskána
- Plotter
- Dataprojektor

37

Poznámky:

.....

.....

.....

.....

VŠE FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Porovnání desktop vs. mobil

PC (desktop)

- Zpracování dokumentů
- Programování
- Stříhání videa
- Zpracování fotografií

Mobilní zařízení

- Bezprostřední komunikace
- Prohlížení obsahu
- Užitečné online aplikace
  - Cestování (navígace)
  - Vyhledávání věcí v okolí
- Poslech hudby, audioknih

Poznámky:

.....

.....

.....

.....

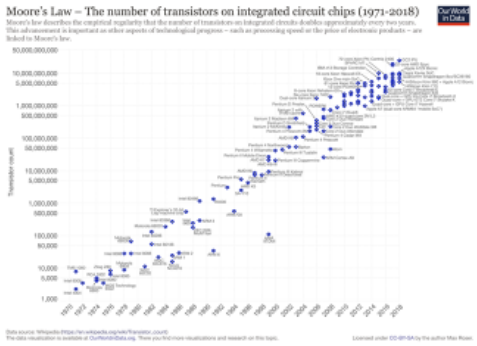
VŠE FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Moorův zákon (1965)

Gordon Moore, viceprezident Intelu

„počet tranzistorů, které mohou být umístěny na integrovaný obvod se při zachování stejné ceny zdvojnásobí zhruba každých 18 měsíců“



Poznámky:

.....

.....

.....

.....

VŠE FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Důsledky Moorova zákona

- Rychlé morální zastarávání výpočetní techniky
- Nutnost častějších investic
- Plýtvání zdroji /ekologie/

Ale taky

- Obrovský pokrok v ICT
- Rozšíření oblastí využití výpočetní techniky (dříve audio, video, nyní voice recognition, VR, AI)
- ICT je motorem inovací
- Čipy se zlevňují a jsou všudypřítomné
- Digitalizace každodenního života

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

Software

Vysoká škola ekonomická v Praze

Poznámky:

.....

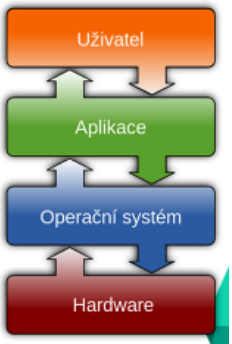
.....

.....

.....

Uživatel – software – hardware

- Hardware – pevné součásti počítače a příslušenství *(počítač, monitor, ale klávesnice, myš, pevné disky…)*
- Software – sada všech programů používaných v počítači/tabletu/mobilu
  - Systémový software (základní software, operační systém)
  - Aplikační software
- Software je
  - Obvykle spustitelný kód, tedy strojové instrukce, které mohou být vykonány procesorem
  - Vše, co není hardware, často je totiž problém oddělit data od softwaru (např. Program zabalený v zip archivu, skript v html kódu webové stránky, makra ve word dokumentu apod.)



Poznámky:

.....

.....

.....

.....

Operační systém

- Základní programové vybavení počítače spuštěné se zapnutím počítače, zůstává v činnosti až do ukončení práce (vypnutí počítače)
- Operační systém počítače plní tři základní funkce
  - Zajišťuje ovládání počítače
  - Zajišťuje abstrakci hardware
  - Zajišťuje správu prostředků
- Obvykle obsahuje grafické uživatelské rozhraní, základní systémové nástroje apod.
- Mimo jiné poskytuje grafické rozhraní pro aplikace; tvůrci aplikací tak nemusí vše jednotlivě programovat (např. Dialogová okna pro práci se soubory apod.), Zároveň je zajištěn jednotný vzhled aplikací

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Firmware

- Ovládací kód pro nízkoúrovňové řízení hardwaru (komunikační zařízení, pevné disky, grafická karta, atd.)
- Je velmi úzce spjat s konkrétním hardwarem (na rozdíl od vysokoúrovňového sw typu operační systém apod.)
- Rozhraní mezi fw a os je ale dnes velmi mlhavé, za fw občas označován např. I OS mobilních telefonů, byť se dnes již o FW v podstatě nejedná, je to spíše historický pozůstatek z doby před chytrými telefony

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Aplikační software

- Programové vybavení počítače
- Grafické nebo textové rozhraní, případně příkazový řádek
- Lze dělit do skupin, byť dělení není disjunktní, typicky ale
  - Kancelářské aplikace, webové prohlížeče, poštovní klienti, komunikační aplikace (skype apod.), Grafické editory, databázové aplikace, ekonomický software, správci souborů, herní aplikace, ...

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Vývoj software

- Zakázkový SW
  - Konkrétní požadavek zákazníka
  - Výhodou přesné pokrytí potřeb podniku
  - Nevýhodou závislost na konkrétním dodavateli, delší doba vývoje
- Typový SW
  - SW běžně dostupný na trhu
  - Často lze doupravit na míru zákazníka (customizace)
  - Běžné aktuální IS
  - Výhodou cena a rychlost
  - Nevýhodou chybějící či nadbytečná funkcionalita

Poznámky:

.....

.....

.....

.....

VŠE FAKULTA INFORMATIKY A STATISTIKY fis.vse.cz fisvse

Verze SW

- V rámci verzí SW se potkáváme s termíny
  - Alfa verze – SW je ve stádiu určeném k testování pouze ve vývojové firmě
  - Beta verze – aplikace je dosud neprodejná, je testována před vlastním prodejem, již se nechává testovat širší skupinou uživatelů (veřejné testování, např. I u zákazníka)
  - Demoverze – již hotové komerční SW, verze určená k vyzkoušení
  - Release candidate – předprodej
  - Final release – určeno k prodeji
  - Trial verze – plnohodnotný SW, omezená doba (podobné jako shareware)

Poznámky:

.....

.....

.....

.....

VŠE FAKULTA INFORMATIKY A STATISTIKY fis.vse.cz fisvse

Licencování softwaru

- Softwarová licence definuje vztah mezi výrobcem a uživatelem softwaru, podmínky použití SW jsou tak definovány licenčním ujednáním
- Každý SW má „nějakou“ licenci
- Nejčastěji to je EULA (end user licence agreement)
  - Jak smí nabyvatel licence produkt používat
  - Nejčastěji v papírové podobě
  - Souhlas s licencí nutný k instalaci produktu

Poznámky:

.....

.....

.....

.....

VŠE FAKULTA INFORMATIKY A STATISTIKY fis.vse.cz fisvse

Licencování softwaru

- Dle obchodního modelu dělíme SW na
  - Komerční software
  - Shareware, adware, freemium (free + premium)
  - Software zdarma, freeware, public domain
- Dle svobody uživatele dělíme SW na
  - Proprietární SW (omezuje svobody uživatele)
  - Svobodný SW (zachovává maximální míru svobod uživatele)

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

proprietární vs. svobodný

- Proprietární
  - Typicky k SW nemáte zdrojový kód
  - Software nemůžete upravovat (i pokud umíte programovat, seženete si programátora)
- Svobodný
  - Neomezuje vás v množství věcí, co s ním můžete dělat

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Svobodný software

- Definovány čtyři základní svobody richardem stallmanem (1984)
  - Svoboda používat program za jakýmkoliv účelem
  - Svoboda studovat, jak program pracuje a možnost přizpůsobit ho svým potřebám
  - Svoboda redistribuovat kopie programu.
  - Svoboda vylepšovat program a zveřejňovat zlepšení, aby z nich mohla mít prospěch celá komunita
- Licenčně ošetřeno prostřednictvím GNU general public license
- Licence požaduje, aby redistribuce byla pod stejnou licencí, což je fakticky ochrannou podmínkou zachování svobodnosti daného SW

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Open-source software

V podstatě se jedná o svobodný software, i když požadavky the open source definition jsou méně striktní než požadavky GNU/GPL, přesto platí:

- Otevřený software je distribuován zdarma včetně zdrojových kódů
- Aplikace je možné libovolně upravovat, často i upravené aplikace dále distribuovat
- Podmínky užívání a redistribuce jsou opět stanoveny v licenčním ujednání
- Open-source aplikace jsou často vyvíjeny programátorskými komunitami

Poznámky:

.....

.....

.....

.....

Komerční software

- Jedná se zpravidla o proprietární software, který je šířen za úplatu
- Podmínky nakládání s komerčním softwarem jsou definovány licenčním ujednáním
- Obchodování s jednou již použitými softwarovými licencemi je v EU legální, viz směrnice EU 2009/24/ES a rozhodnutí soudního dvora EU ze dne 3. 7. 2012

Poznámky:

.....

.....

.....

.....

OEM licence

OEM (original equipment manufacturer):

- Software (nebo obecně zařízení), který je dodáván jako komponenta výrobci třetí stranou (subdodavatelem), výrobce ho může prodávat případně i pod vlastní značkou, každopádně je ale licence vázána na konkrétní dodané zařízení, tedy např. Licence OS na konkrétní počítač
- Takto získanou licenci není možné přenést na jiný počítač, a to ani v případě např. Rozsáhlejší inovace HW

Poznámky:

.....

.....

.....

.....

Shareware

- Proprietární software, který je možné volně šířit a obvykle po předem stanovenou dobu zdarma testovat
- Pro trvalé užívání je třeba zakoupit příslušnou licenci (nebo se případně alespoň registrovat u výrobce)
- Shareware je distribuován často jako volně ke stažení na webových stránkách výrobce nebo jako příbalová CD u časopisů apod., Nejsou to ale výhradní způsoby distribuce

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Freeware

- Je opět proprietární software, který je ale distribuován bezplatně a je možné ho i bezplatně používat
- Podmínky použití jsou definovány opět v licenční smlouvě
- Výrobce může vyzývat uživatele k dobrovolné úhradě formou daru apod.
- Autor si obvykle ponechává autorská práva, k freewaru nejsou dodávány zdrojové kódy, freeware není možné upravovat

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Public domain

- Programy, které je možné zcela svobodně používat, šířit a měnit
- Objevuje se i např. V literatuře či umění – díla, kterým již vypršela autorská práva

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Software as a Service (SaaS)

- Cloudový software
- Software se neinstaluje, používá se na dálku
  - Nevýhoda: bez připojení nefunguje
  - Výhoda: aktualizace není třeba, aktualizuje provozovatel
  - Výhoda: žádná investice do SW

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Cloud computing

- Služby / programy / uložení dat na vzdálených serverech (typicky přes webový prohlížeč, ale ne nutně)
- Public cc – pro kohokoli
- Private cc – pro firmy, vládní složky
- Hybrid cc – kombinace, nejběžnější

59

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Cloud computing

- Saas – software as a service – SW jako služba
  - Data na dálku, SW je v pronájmu
- Paas – platform as a service – platforma j.S.
  - Zaměřeno na vývojáře, možnost vlastních online aplikací, nezávislé na operačním systému
- Iaas – infrastructure as a service
  - Výpočetní infrastruktura, OS, zabezpečení
- Caas – communication as a service
  - Služby spojené s komunikací (telefon - VOIP, e-mail,…)
- Xaas – anything as a a service

60

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Cloud Computing – firmy a

- Google – Gmail, Google Disk, google Apps (kancelářský SW), kalendář…
  - Google App Engine – PaaS
- Microsoft – Office 365
  - Mnoho dalších služeb (komunikace, služby pro firmy)
- Amazon – hosting internetových obchodů
  - Též výpočetní prostředí

61

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Cloud – výhody a nevýhody

- Snížení nákladů (vlastní servery, provoz, údržba, zabezpečení, IT specialisté)
- Jednoduchá centralizace
- Krátká doba implementace

Nevýhody

- Závislost na internetovém připojení
- Ochrana dat
- Monopol poskytovatele

62

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Malware

- Počítačový program určený k získání možnosti vniknutí do počítačového systému nebo k jeho poškození
- Označení je složenina z malicious – zákeřný a software
- Souhrnné označení pro počítačové viry, spyware, adware apod.
- V „lepším“ případě je cílem malwaru získat přístup k výpočetnímu výkonu počítače, v horším případě je cílem např. Poškodit nebo smazat data uživatele apod.

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Adware

- Advertising-supported software
- Součásti software, např. Reklamní sdělení, bannery, změna domovské stránky v internetovém prohlížeči apod.
- Aplikace jsou instalovány se souhlasem uživatele a za jeho vědomí
- Na rozdíl od spyware však nevykonávají žádnou skrytou (často nelegální) činnost

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Spyware

- Software určený ke skrytému odesílání informací z počítače, např. Typu navštívených webových stránek, zadaná uživatelská jména a hesla apod.
- Spyware je typicky šířen jako skrytá součást jiných aplikací
- Z pohledu běžného uživatele může být velmi obtížné rozpoznat, že počítač je takovýmto způsobem napaden

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

Počítačová grafika a multimédia

Vysoká škola ekonomická v Praze

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

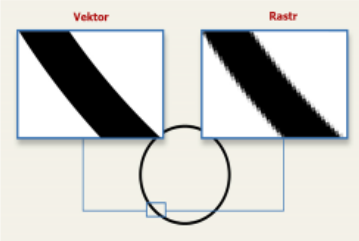
Základní dělení počítačové grafiky

Vektorová grafika

- Obrázek se skládá z objektů

Bitmapová (pixelová, rastrová) grafika

- Obrázek se skládá z bodů



Poznámky:

.....

.....

.....

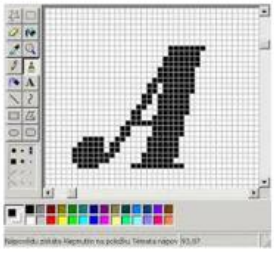
.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Bitmapová grafika

- Obrázek rozložen do malých bodů, pixelů
- Uspořádány do mřížky
- Pixel uchovává informaci o barvě
- Počet pixelů (rozlišení) = kvalita obrázku



Poznámky:

.....

.....

.....

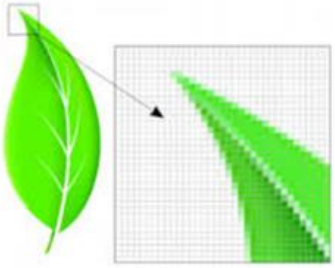
.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Bitmapová grafika – výhody

- Lze zobrazovat i složité předlohy
- Snadné pořízení (např. fotoaparátem, skenerem)



Poznámky:

.....

.....

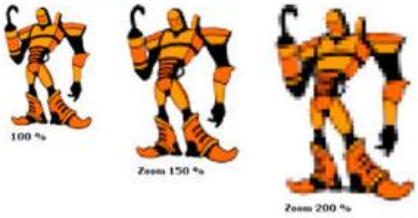
.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Bitmapová grafika – nevýhody



- Velký objem dat
- Ztráta informací při různých úpravách
  - Zhoršení kvality při otočení, zvětšení

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Software pro bitmapovou grafiku

- Malování, IrfranView
  - Spíše pro prohlížení obrázků nebo jednoduché operace
  - Otočení obrázku, výřez
  - Nakreslení jednoduchého obrazce na obrázek
  - Komprese (zmenšení)
- GIMP (svobodný, zdarma)
- Adobe Photoshop (placený, uzavřený)
  - Základní kreslení, výběry, tvary
  - Změna barvy oblasti
  - Úpravy fotografií a barevné filtry
  - Práce ve vrstvách

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Formáty pro bitmapovou grafiku

- jpg, jpeg
  - Rozdělí obrázek na čtverce 8x8
  - Následná komprimace kosinovou transformací
  - Ztráta detailů
  - Kompresní artefakty kolem hran
  - Vhodné pro fotografie
  - Zcela nevhodné pro texty s ostrou hranou
- gif
  - Patentově chráněno, od 1995 potřeba licence
  - Pouze 8 bitů kódování barev (256 barev)
  - Nevhodné pro fotografie
  - Vhodné na obrázky s malým počtem barev
  - Umí animace

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Formáty pro bitmapovou grafiku

- png
  - Patentově nechráněná komprese
  - 1..64 bitů na pixel
  - Umí i průhlednost
  - Nevhodné pro fotografie
  - Vhodné např. pro scanování dokumentů

- bmp
  - Uložení nekomprimovaných dat
  - 1, 4, 8 nebo 24 bitů na pixel
  - Nyní se kvůli velikosti takřka nepoužívá
- tiff
  - Umí s kompresí i bez komprese
  - Lepší než bmp

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Formáty pro bitmapovou grafiku

- psd
  - Formát Adobe Photoshop
  - Podporuje vrstvy a další funkcionality
- xcf
  - Formát GIMPu
  - Podporuje vrstvy a další funkcionality

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Vektorová grafika

- Obrázek se skládá z jasně definovaných objektů
  - (bod, přímka, křivka,...)
- Reprezentace rozměry, umístěním a dalšími vlastnostmi

Poznámky:

.....

.....

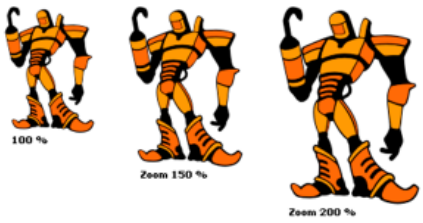
.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Vektorová grafika – výhody



- Libovolné škálování (zvětšení, zmenšení)
- Možno pracovat s objekty samostatně
- Menší paměťová náročnost

Poznámky:

.....

.....

.....

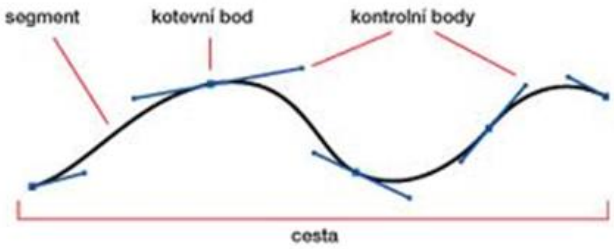
.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Vektorová grafika – nevýhody

- Složitější pořízení obrázku
- Nehodí se pro zápis složitých barevných ploch



Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Software pro vektorovou grafiku

- Svobodný software
  - Inkscape
  - OpenOffice.org Draw
- Proprietární software
  - Adobe Ilustrator
  - CorelDRAW
  - Zoner Draw
- Specializovaný software (nejen vektorová g.)
  - CAD – Computer Aided Design – technické kreslení
  - 3d vektorová grafika

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Formáty pro vektorovou grafiku

Nativní formáty aplikací
- .ai – Adobe Ilustrator
- .cdr – CorelDRAW
- .zmf – Zoner Callisto

Aplikačně nezávislé formáty
- .svg – nativní formát pro Inkscape, webové prohlížeče
- .ps, .eps – postscript (pro tiskárnu)
- .pdf – kontejner, lze vkládat i bitmapy

Formáty různé přístupy k objektům
- Složitější přenositelnost a převod

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Využití

- Bitmapová grafika
  - Fotografie
  - Video
- Vektorová grafika
  - Ilustrace
  - Diagramy a grafy
  - Počítačové animace

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Rozlišení a velikost

- Počet pixelů na jednotku délky vstupu/výstupu
  - dpi = dots per inch (bod na palec)
    - 1 palec = 25,4 mm
  - Pro tisk běžných fotografií – 300 dpi
  - Kvalitní tisk – 600 dpi
- Velikost obrázku = celkový počet pixelů
  - Obvykle v Mpx (megapixel)

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Multimediální kontejnery

Jedna nebo více stop

- Zvuk
- Video
- Text s titulky

Do kontejnerů lze ukládat data v různých formátech

- Stejné zařízení jeden soubor přehraje a jiný se stejném typu kontejneru (stejná koncovka souboru) nikoli

82

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Formáty multimediálních kontejnerů

- avi – zastaralý, od r. 1992, vysoká kompatibilita, digitální fotoaparáty
- mpeg – pracovní skupina Motion Picture Experts Group při ISO. Více formátů a kontejnerů
  - Bitmapová grafika, 24 bitů / pixel, YC_BC_R
  - Max 4096x4096 obrazových bodů, až 30 snímků/s
  - Kosinová ztrátová komprimace až 30:1 obraz, 7:1 zvuk

83

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Formáty multimediálních kontejnerů

- HEIC, HEIF, HEVC – fotoaparáty v mobilních telefonech, obrázky i více obrázků
  - HEIF – i titulky či zvuk
  - HEVC – video (součást MPEG-H), použití DVB-T2
- mp3 – jinak též MPEG-1 nebo MPEG-2
  - Hlavně pro hudbu na počítačích
  - Princip časového a frekvenčního maskování
  - Ztrátová komprese (přibližně na desetinu)
  - Nevhodný pro mluvenou řeč

84

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Formáty multimediálních kontejnerů

- mp4 – MPEG-4 part 14, nástupce avi
  - Menu, více titulků, zvukových stop, 3d objekty
  - Streamování videa, komprese mp3
  - Vychází z něj v mobilech používaný 3GPP (3GP, 3GP2)
- vp9 – otevený formát vyvíjený společností Google, podporují ho internetové prohlížeče, mobilní telefony, tablety, televizory, kamery

85

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Formáty multimediálních kontejnerů

- ogg – projekt pro tvorbu svobodného sw
  - flac – bezztrátová komprese zvuku
  - vorbis, ogg – ztrátová komprese pro hudbu
  - opus – komprese pro řeč
  - speex – nízká kvalita výsledku (malá velikost)
  - ogv – titulky a video
- matroska, mkv, mka, mk3d – otevřený svobodný formát multimediálního kontejneru
  - též soubory MPEG, Vorbis

86

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

RGB vs CMYK

- RGB
  - 3 barevná světla, skládání světel
  - Monitor

- CMYK
  - Na barevné pigmenty svítíme bílým světlem
  - Jisté vlnové délky odrazí a jisté pohltí
  - Vedle cyan, magenta a yellow se doplňuje černá
  - Tisk

Poznámky:

.....

.....

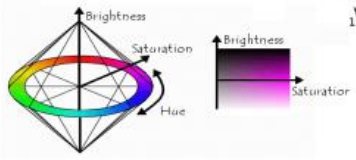
.....

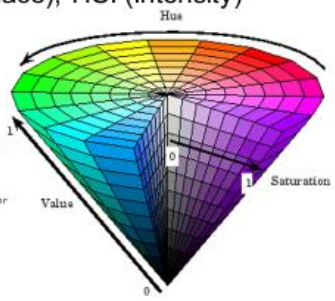
.....

fis.vse.cz fisvse

Další systémy

- HSV – Hue, saturation, value
  - (tón, saturace, jas)
- HSB (brightness), HSL (Luminace), HSI (Intensity)
- YUV, YIQ, YC_BC_R (video)





Poznámky:

.....

.....

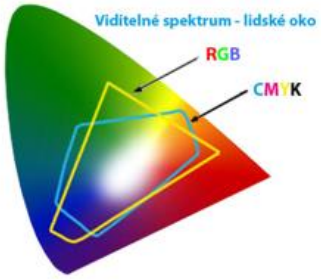
.....

.....

fis.vse.cz fisvse

Barevný gamut

- Barvy dosažitelné v příslušném modelu
- Barvy mimo model – zobrazení jen přibližně
- Gamut zařízení – barvy, které je zařízení schopné zobrazit či zaznamenat
  - Příklad – čistě červená je základ RGB a není v CMYK
  - Při tisku záleží i na konkrétních vlastnostech barvy a papíru



89

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

Podnikové informační systémy

Vysoká škola ekonomická v Praze

Poznámky:

.....

.....

.....

.....

Podnikový informační systém (Enterprise Information System, EIS)

- **Informační systém** je:
  - Využívaný k podpoře řízení,
  - Ke koordinací disponibilních podnikových zdrojů a aktivit,
  - Propojuje podnikové procesy.
- **Účelem** is je:
  - Správa informací a znalostí,
  - Jejich integrace do podnikových procesů,
  - Celistvý pohled na fungování organizace,
  - Zisk a zpracování informací potřebných k manažerskému rozhodování.
- **Cílem** is je:
  - Zvýšení celkové efektivity pracovních procesů,
  - Zvýšení návaznosti pracovních procesů,
  - Zlepšení pracovních návyků a chování uživatelů.

Poznámky:

.....

.....

.....

.....

MRP	MRP II	ERP	ERP II	Postmodern ERP
60. léta 20. stol. vázáno na konkrétní HW	80. léta 20. stol vázáno na konkrétní OS	90. léta 20. stol přenositelnost mezi OS,	začátek tisíciletí integrace aplikací	současnost celostní pojetí IS
sálové počítače	klient-server	třívrstvé aplikace (databáze, aplikace, klientská stanice)	přístup v reálném čase	vícevrstvé systémy, SaaS, Cloud computing
neinteraktivní	přístup přes textový režim	grafické uživatelské rozhraní	multimediální aplikace, webové stránky	mobilní telefony
plánování výroby z pohledu materiálu	řízení výroby, podnikových financí, personalistika	integrovaný IS řízení i nevýrobních podniků	dodavatelsko-odběratelské řetězce, e-business, CRM, BI a další	prozákaznicky orientované systémy
optimalizace skladových zásob	optimalizace výroby	obpimalizace podniku	aktivace hodnotového řetězce	komplexní přístup k digitální transformaci
jeden systém	modulární systém	systém na míru společnosti	propojené systémy	balíkové systémy pro různé typy podnikání

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Oblasti systémů postmoderního ERP

- Finance (ekonomika)
  - Účetnictví vč. Manažerského
  - Správa podnikových aktiv (EAM, Enterprise Asset Management)
- Řízení lidských zdrojů (HRM, Human Resource Management)
  - Pracovní doba, mzdy, školení, benefity
  - Komunikace, výměna informací

93

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Oblasti systémů postmoderního ERP

- Výroba, logistika, provoz či projektování (dle typu podniku)
  - Řízení kvality a procesů, jakosti, IT
  - Plánování výroby, zásob, skladu
  - Řízení dodavatelského řetězce
    - SCM – Supply Cahin Management
    - SRM – Supplier Relationship Management
  - Správa majetku

94

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Oblasti systémů postmoderního ERP

- Marketing a prodej
  - Informace o výrobcích a službách
    - PIM – Product Information Management
  - Řízení vztahů se zákazníky
    - CRM – Customer Relationship Management
      - Zpracování zakázek
  - Cenová politika
  - Řízení objednávek, zpracování zakázek
  - Servis

95

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Základní moduly / systémy

- BI – Business Intelligence – manažerský informační systém určený pro rozhodování
- CRM – Customer Relationship Management – řízení vztahu se zákazníky, může být součástí BI
- SCM – Supply Chain Management – řízení dodavatelského řetězce
- Častá kombinace – HRM + EAM + ECM (správa obsahu, Enterprise Content Management)

96

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Nejznámější výrobci ERP

- SAP
- Oracle Corporation
- Infor
- Microsoft
- Asecco Solutions
- Další výrobci
  - IBM
  - ABRA

SAP - První verze ERP v 70. letech
- Různé operační systémy a různé databáze
- SAP NetWeaver – internetově orientované
- SAP Business One – pro střední a malé firmy
- Nejrozšířenější SAP R/3 s množstvím modulů:
  - Finanční účetnictví, kontroling, evidence majetku, plánování dlouhodobých projektů, řízení oběhu dokumentů, management kvality…

ORACLE
- Společnost zaměřená primárně na Systémy řízení báze dat
- Oracle ERP
  - Oracle e-Business Suite
  - Oracle JD Edwards Enterprise-One
  - Oracle Cloud ERP

- Microsoft Dynamics NAV
  - Pro středně velké společnosti
- Microsoft Dynamics 365 Business Central
  - Cloudové řešení
  - Pro malé, střední i začínající podniky

97

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

eGovernment

Vysoká škola ekonomická v Praze

Poznámky:

.....

.....

.....

.....

eGovernment

- Využití informačních a komunikačních technologií s cílem zlepšit a nebo posílit účinnost a efektivitu poskytování služeb ve veřejném sektoru.
- eGovernment je využívání informačních technologií veřejnými institucemi pro zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi za účelem zvyšování efektivity vnitřního fungování a poskytování rychlých, dostupných a kvalitních informačních služeb

Poznámky:

.....

.....

.....

.....

Komunikační kanály (složky) eGovernment-u

- G2C (Government to Citizens)
- G2B (Government to Businesses)
- G2E (Government to Employees)
- G2G (Government to Governments)
- C2G (Citizens to Governments)

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

eGovernement - úskalí

- Koexistence ne-elektronické a elektronické komunikace
- Rovný přístup všech obyvatelů k elektronickým službám
- Bezpečnost
- Ochrana před zneužitím

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

eGovernement - úskalí koexistence

- Listinná<->digitální podoba dokumentů
- Ověřování listinných<->digitálních dokumentů
- Ruční<->digitální podpis
- Ověřený ruční<->digitální podpis
- Fyzická<->elektronická identita (autentizace)
- Ověření fyzické<->elektronické data a času

Nejen prakticky a technologicky ale i právně.

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Přístup k informacím, komunikace

- Informativní webové portály
- Datové schránky
- Základní registry veřejné správy
- Czechpoint
- Elektronický podpis

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Datové schránky

- ISDS – informační systém datových schránek
- Informační systém veřejné správy
- Zřízené dle zákona č. 300/2008
- Elektronické úložiště zvláštního typu
- Zřizuje a spravuje ministerstvo vnitra české republiky
- Provozovatelem je držitel poštovní licence (česká pošta)

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Datová zpráva

- Obálka obsahující
  - Elektronickou značku (e-razítko)
  - Časovou značku (kvalifikované časové razítko)
- Tělo zprávy
  - Forma příloh
  - Chybí „klasické“ tělo zprávy jako u e-mailu
- Po vložení zprávy (příjemce)
  - Avízo SMS (za poplatek)
  - Na mail (bezplatně)

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Vlastnosti datových schránek

- Neomezená velikost
- Doručenka – potvrzuje doručení, přečtení, fikci doručení
- Dokumenty zůstávají v schránce po dobu 90-ti dnů od přečtení
- Pro delší platnost
  - Uložení v datovém úložišti (je opatřena časovým razítkem i elektronickým podpisem)
  - „Datový trezor“ (placené)
  - Převést do listinné podoby (autorizované pracoviště, placené)

Poznámky:

.....

.....

.....

.....

Technické řešení

- Webové rozhraní – https://mojedatovaschranka.Cz
- Protokol SOAP nad HTTPS (napojení spisových služeb firem a další)
- Mnoho dalších SW pro komunikaci s datovými schránkami – proprietární i svobodný SW
  - Viz např. Wikipedie heslo datové schránky

Poznámky:

.....

.....

.....

.....

Právní úprava elektronických úkonů

- Závaznost – právní váha úkonu pomocí datové schránky je stejná, jako kdyby byl učiněn písemně do vlastních rukou
- Garantované doručení – datová zpráva, která je pomocí schránky odeslána, je garantovaně doručena příjemci. Za doručení se považuje okamžik, kdy se do datové schránky adresáta přihlásí oprávněná osoba
- Právní fikce doručení – pokud se do 10 dnů adresát do schránky nepřihlásí, zpráva je uplynutím této lhůty považována za doručenou, aniž ji příjemce otevřel – mimo případ náhradního doručení (překážka do 15-ti dnů)
- Pomíjivost – zprávy jsou ze schránky automaticky odstraněny po 90 dnech od doručení
- Pokuty 10M za nevyžádaný dokument, 20M za škodlivý SW

Poznámky:

.....

.....

.....

.....

Datové schránky bezpečnost

- Chráněna ID a heslem (5 pokusů pak 1 hodinu deaktivována, info uživateli)
- Po 30-ti minutách neaktivity – automatické odhlášení
- Vyšší úroveň – jednorázové heslo (premium SMS nebo jednorázový bezpečnostní kód)
- Lze nainstalovat mobilní klíč ISDS (za zvláštních podmínek)
- Lze použít čip na eobčance
- Lze použít autentizační certifikát
- Schránka má pouze tyto stavy: funkční , neexistuje, znepřístupněna, zrušena

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Informační systém základních registrů (ISZR)

- Správcem ministerstvo vnitra,
- Čtyři registry
- Provozovatelem správa základních registrů

ORG – převodník identifikátorů fyzických osob

- Správcem je úřad pro ochranu osobních údajů,
- Ochrana osobních údajů v registrech,
- Nepoužívá se rodné číslo,
- V každém systému subjekt jiný identifikátor
- V ORG pouze identifikátory a nikoli další údaje o subjektu

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Registry

- Registr osob (ROS)
  - Správcem je český statistický úřad,
  - Eviduje údaje o právnických osobách (PO), fyzických osobách - podnikatelích (FO) a orgánech veřejné moci (OVM).
- Registr obyvatel (rob)
  - Správcem je ministerstvo vnitra,
  - Eviduje aktuální referenční údaje o občanech ČR, cizincích s povolením k pobytu nebo zahraničních vlastnících nemovitostí.

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Registry

- Registr územní identifikace adres a nemovitostí (RUIAN)
  - Správcem je český úřad zeměměřický a katastrální (ČÚZK),
  - Eviduje údaje o základních územních prvcích, např. Území států, krajů, obcí nebo částí obcí, parcel či ulic.
- Registr práv a povinností (rpp)
  - Správcem je ministerstvo vnitra,
  - Eviduje údaje o působnosti orgánů státní moci, právech a povinnostech osob

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

CzechPoint

- Czech POINT neboli český podací ověřovací informační národní terminál,
- Asistované místo výkonu veřejné správy
- Každý člověk může získat všechny informace o údajích, které o něm vede stát v centrálních registrech
- Lze učinit podání ke státu.
- Https://www.Czechpoint.Cz/

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

CzechPoint

- Ověřené výstupy
  - Z živnostenského rejstříku,
  - Z obchodního rejstříku,
  - Z katastru nemovitostí,
  - Z rejstříku trestů
- Další služby:
  - Ověření podpisu
  - Ověření dokumentu
  - Zaslání zprávy do datové schránky
  - Konverze dokumentů z a do datové schránky
- Více viz https://czechpoint.Cz

Poznámky:

.....

.....

.....

.....

FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Czech Point – kontaktní místo

- Automaticky
  - Notáři a exekutoři
  - Orgány veřejné moci (základní registry)
- Na žádost (většinou mají)
  - Úřady
  - Ambasády (velvyslanectví, generální konzulát)
  - Česká pošta
- Další
  - Banky, advokáti

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Autorizovaná konverze dokumentů

- Autorizovaný převod dokumentu do elektronické podoby
- Ověřuje se elektronickým podpisem provádějící instituce
- V ČR přesně specifikováno, kdo smí provést (např. Czech POINT)
- Elektronická forma se považuje za ověřenou kopii listinné podoby (stejné právní účinky jako originál)

Poznámky:

.....

.....

.....

.....

VŠE / VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE

IT Governance (ITG)

Repetitorium

4SA310

Ing. Richard A. Novak, Ph.D.

VŠE/FIS/KSA Praha

Poznámky:

.....

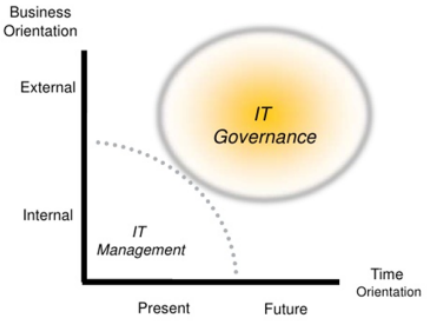
.....

.....

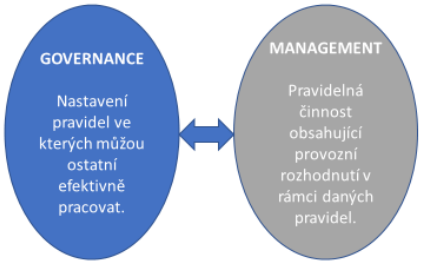
.....

IT Governance **vs** Management

Graf 1:



Graf 2:



2

Poznámky:

.....

.....

.....

.....

IT Governance vs Management

Co je Governance?

I. Governance = vláda, správa .... Stanovení pravidel
   I. Ústava, Zákony .... atd. = U státu
   II. Zakladatelská a Společenská smlouva ....atd. = U Firmy

II. Governance obecně představuje řídící rámec definující role, zodpovědnosti, pravomoci a způsob komunikace

III. Součástí je také měřící a kontrolní systém
   I. Performance management vs Audit
   II. Risc Management

IV. Cílem je vybavit organizaci/firmu jasně definovanými pravidly pro efektivní plnění cílů

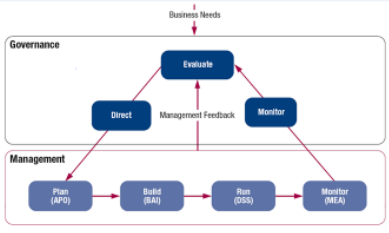
V. IT Governance = stanovení pravidel pro řízení IT
   - Evaluate, Direct, and Monitor (EDM) covers the governance activities (COBIT)

Co je Management?

I. Strategie (Gov) x Taktika (Mgt) x Operativa (Mgt)

II. Management vezme zadání vlastníků a snaží se ho provést v praxi
   I. Executive Management

- Plan, Build, Run, and Monitor
  - (PBRM) covers the management activities. (COBIT)



3

Poznámky:

.....

.....

.....

.....

IT Výzvy — Oddělení role Vlastníka a Manažera

I. Kdo je typický členBoard of Directors? (česky Představenstvo)
   I. Členy Představenstva vybírá vlastník nikoliv CEO.
   II. Člověk, který dříve působil v Executive management (CEO..) a má velkou diverzitu zkušeností (Sales, Marketing, Operation, Finance, Právo..etc)
   III. Člověk, který má dlouhý a známý „track record" ze kterého vyplývá, že se mu dá věřit. (Trust and Transparency)

II. Co se očekává od člena Představenstva?
   I. „Challengingthe Executive Management" …. Zejména klást dobré otázky a naslouchat odpovědím CEO a CxO.
   II. „Manage the Risk" ….. Pravidelně číst reporting a audit zprávy.
   III. „Steering on long term & strategiclevel" …… Co Vývoj trhu? Co naše Konkurenční Výhoda? Jaký je plán na 1,3,5,10 let?

III. Jaká je role IT z perspektivy členů Představenstva?
   I. Zásadní což se změnilo za posledních cca 5 let!
   II. Bývala to podpůrná oblast a dnes je toCORE pro úspěch firmy na trhu?
   III. Většina firem musí projít Digitální transformací a není na to připravena, takžeBoard musí „Challenge & Control IT"

Nástroje Vlastníka = Dobré otázky a naslouchání (Audit)

Nástroje Managementu (CEO,CxO) = Chain of Command, Carrot & Stick..etc.

4

Poznámky:

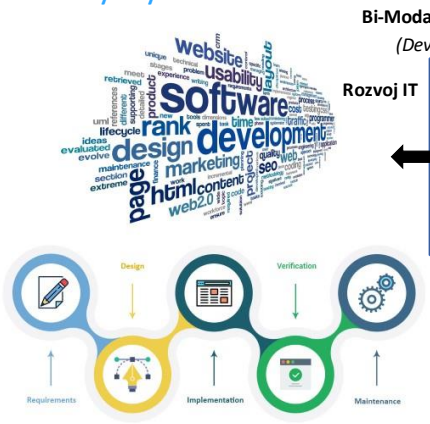
……

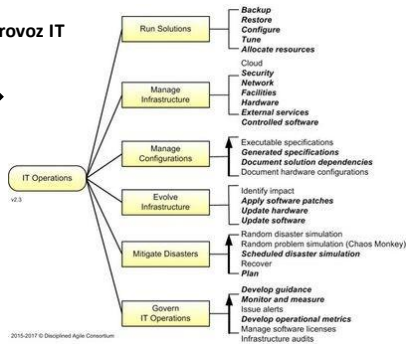
……

……

……

IT Výzvy — IT Rozvoj a Provoz





5

Poznámky:

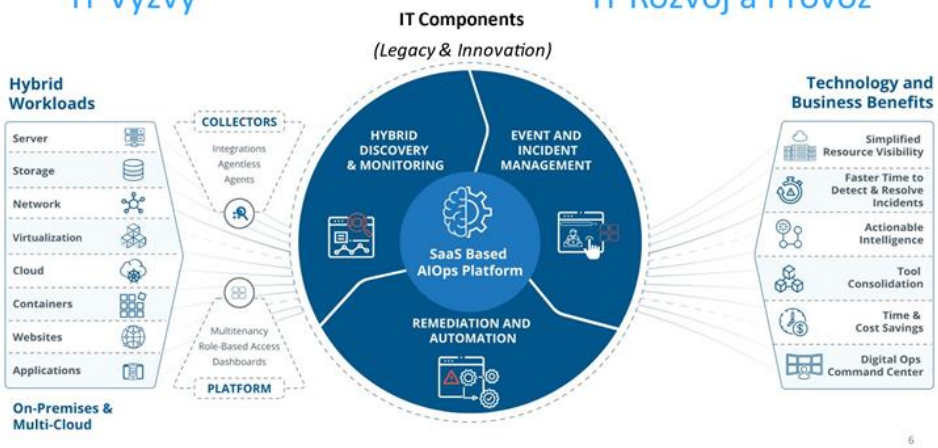
……

……

……

……

IT Výzvy — IT Rozvoj a Provoz



6

Poznámky:

……

……

……

……

Základní Pojmy — Governance

Corporate (Enterprise) Governance

- Představuje systém, kterým je vedena a kontrolována CELÁ společnost
- Systém definuje distribuci práv a povinností mezi zainteresovanými stranami společnosti jako jsou akcionáři, výkonný management, statutární orgány, zaměstnanci a zákazníci, případně dal zainteresované osoby.
- Jedná se o soubor právních a exekutivních metod a postupů, které zavazují především veřejně obchodovatelné společnosti udržovat vyvážený vztah mezi společností a těmi osobami jež ji tvoří.

Vazba Corporate & IT Governance

- IT Governanceje podmnožinou a nedílnou součástí Corporate Governance
- Pří řízení společnosti rozlišujeme různé úrovně Governance
  - Corporate Goverance (CG)
  - Enterprise Governance (EG)
  - Enteprise Governance of IT (EGIT)
  - Project Governance
  - Security Governance
  - …etc.

7

Poznámky:

.....

.....

.....

.....

Základní Pojmy — Audit … EGIT

Postupný vývoj od Auditu k EGIT **:**

- Do r. 1996: Audit IT– jak zjistit co IT dělá a co má
- Do r. 1998: Řízení IT– Co má management od IT očekávat
- cca r. 2000: Výkonnost IT- Management řeší jak změřit výkonnost IT
- cca r. 2005: ITGovernance – Zavádění pravidel pro IT
- cca r. 2012: EGIT komplex- Těsné propojení IT s byznysem

8

Poznámky:

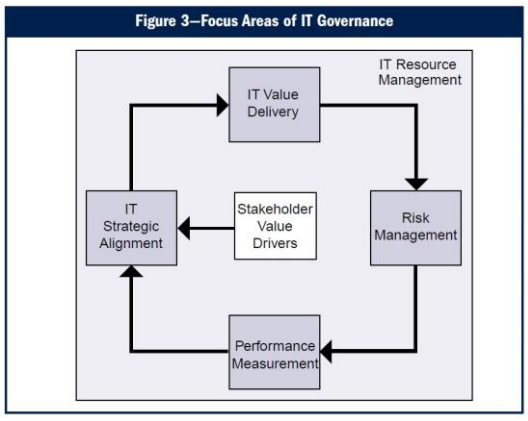
.....

.....

.....

.....

Základní Pojmy — EGIT a Klíčové oblasti



Komentář:

- Dle ITGI
  - Board Briefing on IT

9

Poznámky:

.....

.....

.....

.....

Základní Pojmy — Očekávání od EGIT

EGIT rámec (Framework)

Rámec EGIT (např. dle COBIT 5) pokrývá všechny požadované procesy a IT zdroje tak aby IT vhodně podporovalo společnosti při vytváření hodnot a naplňování očekávání zainteresovaných osob.

Zainteresovaní (Stakeholders) očekávají od implementace EGIT především:

- Zvýšení transparentnosti mezi akcionáři, výkonným a IT managementem (kaskádování cílů)
- Dosažení souladu s relevantními zákony, regulacemi a politikami
- Nastavení kontrolních mechanismů a reportingu
- Vytváření vyšší přidané hodnoty z IT a svěřených zdrojů
- Včasná identifikace a eliminace rizika vyplívající z IT
- Zlepšení řízení IT v souladu s „best practice"

10

Poznámky:

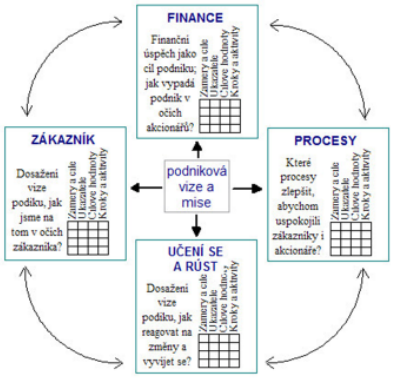
.....

.....

.....

.....

Propojení Byznysu a IT — Enterprise BSC



Komentář:

- **Balanced Score Card (BSC)**,
- česky **Systém vyvážených ukazatelů výkonnosti podniku**, je metoda v managementu, která vytváří *vazbu mezi* **strategií** a **operativními činnostmi** *s důrazem na měření výkonu.*
- Autory metody publikované od roku 1992 jsou Robert S. Kaplan a David P. Norton.

11

Poznámky:

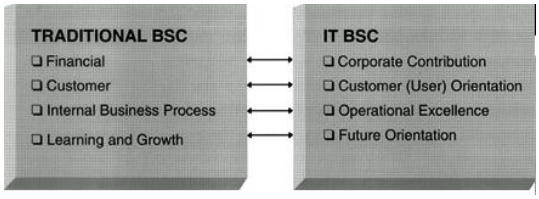
.....

.....

.....

.....

Propojení Byznysu a IT — IT BSC



Komentář:

- Většinou se **v praxi s BSC pracuje formou tabulky** kam se krom cílů **(Objectives)** doplňují také měřitelné metriky **(Measures),** cílová hodnota těchto metrik **(Targets)** a hlavně projekty a aktivity, které my měli tyto cíle a jejich dosažení zajistit tedy **(Initiatives).**

12

Poznámky:

.....

.....

.....

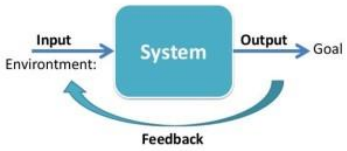
.....

Systémové metody řízení — Úvod do Teorie systémů

Definice systému

„Systém (či soustava) je celek složený z částí, které na sebe vzájemně působí. Mezi částmi systému mohou probíhat toky informací, hmoty a energie.“

Rozdělení systémů:



- Systémy můžeme dělit podle následujících kritérií:
- **uzavřené × otevřené** – podle toho, zda nastává interakce s okolím
- **deterministické× stochastické** – podle toho, zda systém vykazuje jednoznačné nebo náhodné (statisticky popsatelné) chování,
- **statické × dynamické** – podle toho, zda se vyvíjejí v čase,
- **spojité × diskrétní** – podle toho, zda se hodnoty mění spojitě nebo skokově,
- **tvrdé × měkké** – tvrdé systémy jsou spojovány s dobře strukturovanými problémy (řešení lze poměrně snadno algoritmizovat), naopak v měkkých systémech vystupuje celá řada faktorů, jejich struktura není přesně definována, údaje jsou neurčité a neúplné

13

Poznámky:

.....

.....

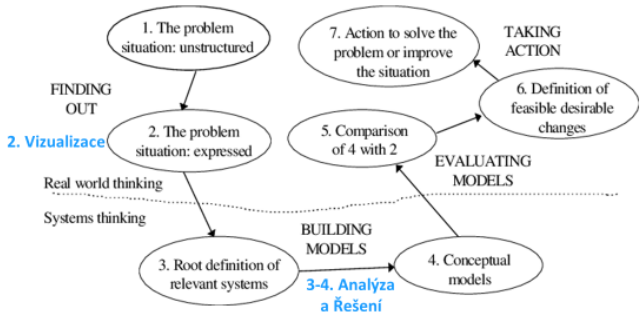
.....

.....

Systémové metody řízení — Rich Picture

Měkké Systémové Metodologie (SSM)

- Soft systems methodology (SSM) is an approach to organizational process modelling (business process modelling) and it can be used both for general problem solving and in the management of change.



Peter Checkland

- Metodologie, která uvažuje 7 kroků.
- Důležité jsou zejména body **Vizualizace a Řešení 2..4.**
- Pro **bod 2** lze použít tzv. **Rich Picture.**

14

Poznámky:

.....

.....

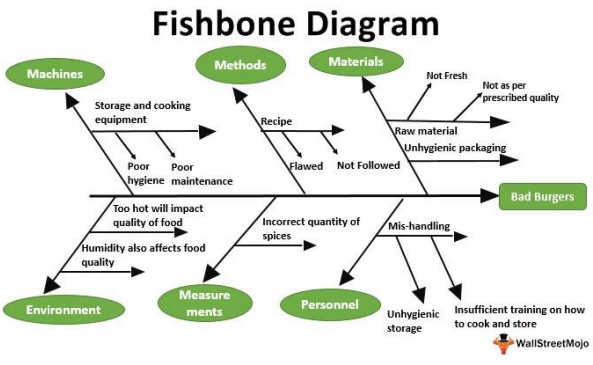
.....

.....

Systémové metody řízení — Fishbone Diagram

Fishbone diagram

- Metoda Rybí páteře
- Hlava ryby je hlavní problém
- Kosti jsou dílčí faktory Příčiny a Důsledky (agregated) do oblastí.
- V IT vhodné pro Root-Cause Analysis technických problémů



15

Poznámky:

.....

.....

.....

.....

Systémové metody řízení — Occamova břitva

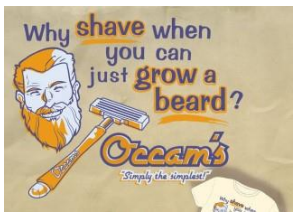
Dobré otázky jsou základní nástroj Vlastníka i Manažera!

6x Proč?

- Co se stalo?
- Kdo to viděl?
- Co jste viděl?
- Co si myslíte, že se to stalo?
- Máte nějaké jiné vysvětlení?
- Jaké z toho vyvodíme opatření?

Occamova břitva

- Základní vědecký přístup
- Mezi řešení situace, které dávají stejný výsledek je nejlepší vybrat to nejednoduší.



Prioritizační otázky

- Týká se to nás?
- Můžeme s tím něco dělat?
- V jaké čase jsme schopni to řešit?
- Umíme o tom shromáždit údaje?
- Opravdu to chceme řešit?

Paretovo pravidlo

- 80% problémů způsobuje 20% faktorů.

16

Poznámky:

.....

.....

.....

.....

Systémové metody řízení — Řízení Podniku a IT

Je rozdíl jestli řídím stroje nebo lidi anebo jejich kombinaci!

Řízení Podniku a IT útvaru je velmi komplexní systém.

Teorie Systémů tvoří základ pro všechny metody uplatňované **Governance i Management** oblasti.

17

Poznámky:

.....

.....

.....

.....

Úvod do COBIT

1) **Manažeři (Top-Down)**
   1) TOP manažeři
   2) Strategičtí manažeři podniku
2) **IT Auditoři**
   1) Speciální kategorie a Certifikace
3) **Ostatní uživatelé**
   1) Vlastnící
   2) IT & Security Specialisté

Kdo je uživatelem?

18

Poznámky:

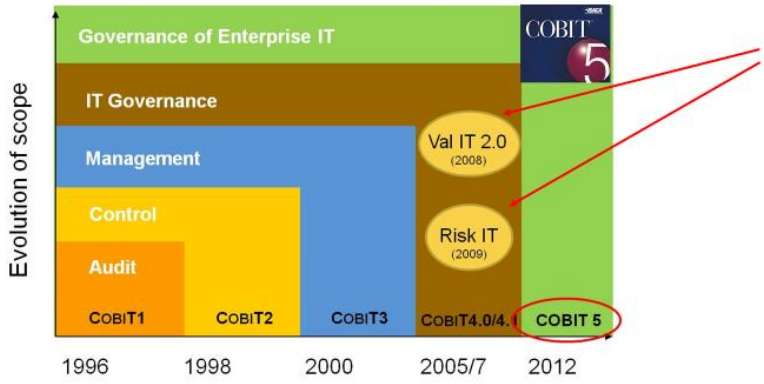
.....

.....

.....

.....

Úvod do COBIT — Vývoj v čase



19

Poznámky:

.....

.....

.....

.....

Představení COBIT — Core Publications

- **COBIT 5 / Framework**
  - A Business Framework for the Governance and Management of Enterprise IT ..... (*The theory).*
- **COBIT 5 / Enabling processes**
  - Main Guide for users of COBIT 5. *(All Process covered here)*
- **COBIT 5 / Implementation**
  - The method for continual improvement *(lifecycle & change management)*

20

Poznámky:

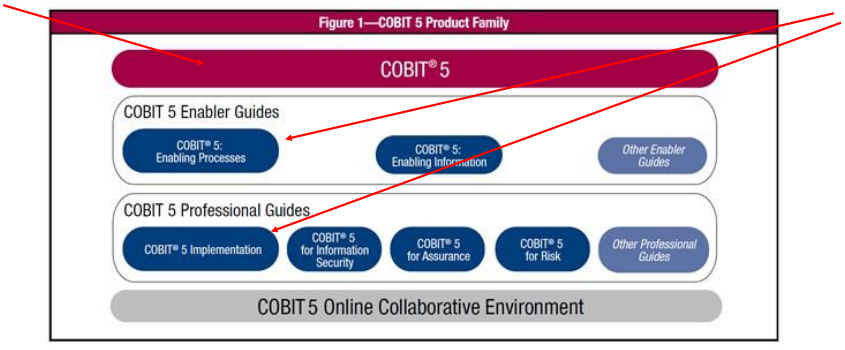
.....

.....

.....

.....

Představení COBIT — Product Family



21

Poznámky:

.....

.....

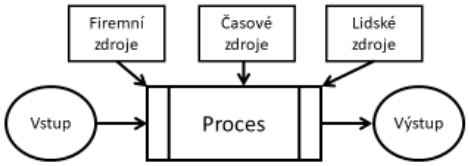
.....

.....

Základy Procesního řízení

Co je proces? (Obecně):

- **Proces** je účelně naplánovaná a realizovaná posloupnost činností, ve které za pomoci odpovídajících zdrojů probíhá transformace vstupů na požadované výstupy.



24

Poznámky:

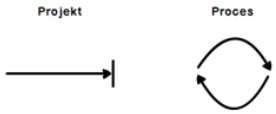
.....

.....

.....

.....

Základy Procesního řízení



Procesní vs Projektové řízení

- **Proces** (z latinského „processus" – postupovat, vyvíjet se) se v managementu používá pro posloupnost činností, které na sebe navazují. Tyto činnosti se opakují a jednotlivé části lze popsat.
  - **Smyslem procesního řízení v organizaci je dosáhnout efektivity u opakujících se činností.**
- **Projekt** (z latinského „pro-jicio, pro-iectum" – návrh, rozvrh) **se používá pro jednorázovou změnu**. Průběh těchto projektů bývá unikátní, obvykle se ho účastní více lidí a dopředu nelze přesně popsat, předpovídat činnosti, které bude nutno provést.
- S trochu zjednodušení lze tedy říct, že procesní řízení se v managementu používá na opakované, snadněji popsatelné činnosti (výroba, nákup, prodej, ...) a projekty na jednorázové a složitější řízené změny (zavedení nového informačního systému, ...)

Co mají procesní i projektové řízení společné je, že obojí by mělo mít definovaný cíl.

25

Poznámky:

.....

.....

.....

.....

Základy Procesního řízení

Dělení podnikových procesů:

Podnikové procesy dělíme dle jejich vlastností do tří skupin na:

- **Hlavní - Řídící – Podpůrné** procesy

Vlastnost / Typ Procesu	Hlavní proces	Řídící proces	Podpůrný proces
Přidává proces hodnotu?	Ano	Ne	Ano - Ne
Probíhá proces napříč společností?	Ano	Ano - Ne	Ne
Má proces externí zákazníky?	Ano	Ne	Ne
Generuje proces tržby?	Ano	Ne	Ne

- **IT Proces** patří mezi podnikové proces a to nejčastěji podpůrné.

26

Poznámky:

.....

.....

.....

.....

Základy Procesního řízení

Zralost Procesu a CMMI (pohled na kvalitu - efektivitu)

neexistující – není žádný pozorovatelný proces; organizace dosud neměla potřebu situaci řešit. Při výskytu události reaguje spontánně.

náhodný – organizace vnímá potřebu situaci řešit, ale veškeré aktivity se provádějí na ad-hoc a individuální bázi.

opakovaný – snaha o vytvoření standardních postupů, ale jejich využití je intuitivní nikoliv povinné a prováděné vyškolenými lidmi.

formalizovaný – proces je popsán, zaměstnanci vyškoleni a znají svoje role.

měřitelný – je přidán proces měření výkonnosti procesu a řízení (zlepšování).

optimalizovaný – po mnoha iteracích jde o „best practice" a „continual improvement"

27

Poznámky:

.....

.....

.....

.....

Základy Procesního řízení

Zlepšování Procesu (Příklady a Opatření)

Eliminace zbytečných činností, např. netvořících přidanou hodnotu

Paralelizace činností, vyšší výkon a odstranění lineární závislosti

Centralizace zdrojů a jejich správy, vyšší úspory a kontrola

Spojování činností, které eliminuje zbytečné vazby (interface) mezi operacemi

Jediné kontaktní místo pro zákazníka procesu, Front and Back Office

Delegace pravomocí, posun rozhodování na nižší úroveň a tím zrychlení

Zvýšení důvěry mezi kooperující podniky/útvary/pracovníky a tím snížení kontrol

Zvýšení úrovně znalostí pracovníků a jejich motivace

Automatizace, činnost je plně nebo částečně realizovaná strojem či SW

28

Poznámky:

.....

.....

.....

.....

Business Proces Management BPM

Business Proces Management česky *(Procesní řízení)*

Jedná se o **manažerskou disciplínu i technologii** opřenou o uchopení struktur firmy, její architektury a jejího řízení prostřednictvím podnikového modelu („**Enterprise Model**"). Ten musí zachytit základní rozměry podnikání:

- *jeho cíle*
- *hodnototvorné procesy*
- *jejich organizační, znalostní i informační infrastruktury a podpůrné technologie*

- *obsahuje řadu metod a nástrojů, které jsou buď obecné nebo komerční povahy*
- Dvě základní Notace (formy zápisu procesu)
  - **BPMN 2.0**
  - **EPC**

29

Poznámky:

.....

.....

.....

.....

ITIL úvod

1) Evoluce ITIL od v2 do v3 a v roce 2019 v4 *(SW, AI, Agile & Lean..etc)*

30

Poznámky:

.....

.....

.....

.....

ITIL 3 - Základní oblasti

- **ITIL v3**
- **Lifecycle view**
- 5 service lifecycle stages. These are 26 processes in total in domain stages:

1. *Service Strategy*
2. *Service Design*
3. *Service Transition*
4. *Service Operations*
5. *Continual Service Improvement (CSI)*

31

Poznámky:

.....

.....

.....

.....

ITIL 4 Introduction

- ITIL 4 is very comprehensive now but still the core is about:
  - IT Service Management *(customers)*
  - Processes / Practices
  - Products & Services
- It reflects the changing IT world
  - **Increasing complexity**
    - External factors, Customers and Suppliers participation
  - **New IT trends** above infrastructure such are
    - SW dominance
    - Agile, Lean & DevOps approaches
  - **Focus on Benefits rather then technology**
    - Aligning IT with business strategy
    - Value creation

32

Poznámky:

.....

.....

.....

.....

Organizační modely

1) **Základní funkce / procesy managementu**
   1) **Plánování**
      - Když je znám cíl akcionáře tak je potřeba stanovit dílčí aktivity v čase, které zajistí naplnění cíle.
   2) **Organizování**
      - Identifikace činností (procesů řízení) vedoucích k dosažení plánem stanovených cílů a k zajištění potřebných zdrojů.
   3) **Personální zajišťování**
      - Obsazování pracovních pozic těmi správnými lidmi.
   4) **Vedení a Motivace**
      - Leadership a Komunikace
   5) **Kontrolování**
      - Zjišťování odchylek mezi plánem a skutečností, analýza příčin a přijetí korektivních opatření.

33

Poznámky:

.....

.....

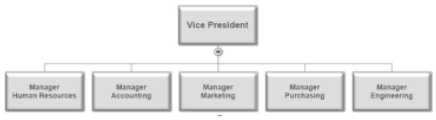
.....

.....

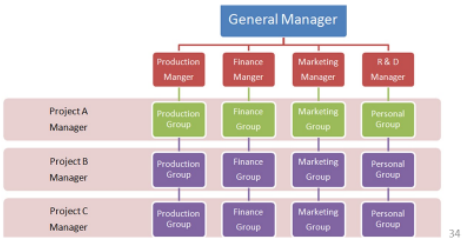
Organizační modely

Základní dělení - Organizační modely

- **Stabilní struktura**
  - *Liniově (Funkční)*
  - *+ Štáby (Experti a Poradci)*



- **Flexibilní struktura**
  - *Maticové a Projektové řízení*



34

Poznámky:

.....

.....

.....

.....

Alternativní Organizační modely

Crowdsourcing a Svobodná firma

35

Poznámky:

.....

.....

.....

.....

Komunikace

Jak souvisí Management a Governance s komunikací?

Základní nástroj managera či vlastníka je:

I. **naslouchání** pro **získání informací** *(původ slova Audit)*

II. **Pro zadávání úkolů** je to pak specifikace úkolu a jeho **komunikace zadání na team** a podřízené tak aby ho plně pochopili a byly schopni **splnit bez „zkreslení“.**

36

Poznámky:

.....

.....

.....

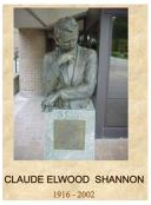
.....

Informační model podniku

Teorie Informace

Teorie Informace / C.E. **Shannon**

- Základy v roce 1948 a práce Matematická Teorie Sdělování
- Zavedl Pojmy, které vedly ke vzniku Telekomunikaci a IT:
- **Entropie**
  - Míra informace tedy Míra Neuspořádanosti či Míra Neurčitosti
- **Množství Informace**
  - Pří růstu informace klesá entropie a při Odstranění neurčitosti se získá informace (Big Data)
- **Rychlost Přenosu zpráv**
  - Metody vzorkování, kódování a chybovost



37

Poznámky:

.....

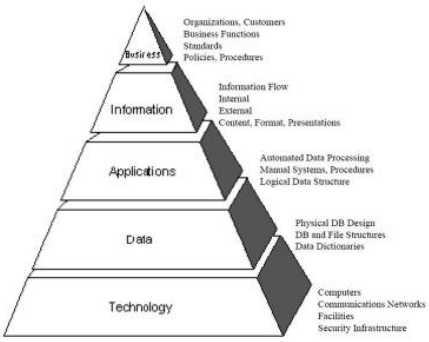
.....

.....

.....

Informační model podniku

Informace a Mgmt.



- **Informační model podniku**
  - Vhled jako uspořádání pyramidy
- Enterprise Information model
  - Pyramidal View

38

Poznámky:

.....

.....

.....

.....

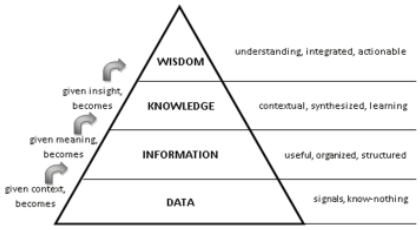
Informační model podniku

Informace a Mgmt.

Data
neboli **fakta popisují** nezaujatě (bez interpretace) objektivní **realitu.**

Informace
„informare", latinsky znamenající informovat.
Ve středověké filozofii tento termín znamenal "dát formu myšlence". "Je tedy zřejmé že už od samého vzniku toto slovo popisovalo určité zhmotnění dat do myšlenky a **významu jenž se dá interpretovat** a komunikovat.

Znalosti (Moudrost)
Aktivní porozumění určité situaci (realitě). Výsledek a uchopení procesu učení jenž se dá použít **pro praktické rozhodovací situace.**



39

Poznámky:

.....

.....

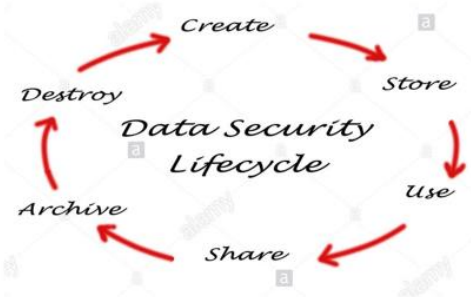
.....

.....

Informační model podniku

Informace a Mgmt.

Data Security Life-cycle:



40

Poznámky:

.....

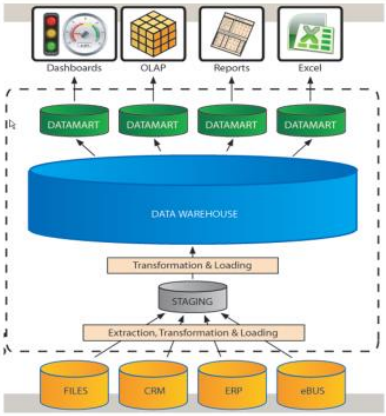
.....

.....

.....

Informační model podniku

Data & IS view



- DW, One version of true – for management
- Business Inteligence – for all users
- Datamarts – per functional units
- ETL and Staging – for data processing
- Transactional Systems – data sourcing

41

Poznámky:

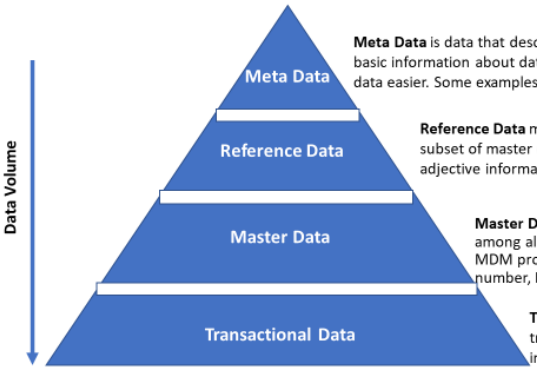
.....

.....

.....

.....

Informační model podniku — Data & IS view



Meta Data is data that describes other data. It is used to summarize (aggregate) basic information about data which can make tracking and working with specific data easier. Some examples include: Sum, Average, Time and date of creation..etc.

Reference Data management (RDM) can be thought of as a specialized subset of master data management (MDM). It is reference and adjective information to MD. E.g. Title, Role, Category...etc.

Master Data are key (Golden) data of IS that are hared among all systems and managed by special Governance and MDM process. E.g. Customer Name, Address, Phone number, Product ID or Name..etc.

Transactional Data are produced often as a stream from transactional systems (by Humans or Machine). E.g. EDR in Telco, or Banking, Sold product in Retail..etc.

42

Poznámky:

.....

.....

.....

.....

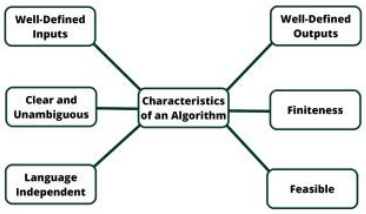
Informační model podniku — Decision Supporting Systems (DSS)

Machine Learning / Expert Systems / AI

- *ML / Data First, Algorithm second*
- *ES / Aggregated Knowledge of Experts*
- *AI / supervised vs self-learning AI...etc*

Algorithm Definition:

In mathematics and computer science, is a finite sequence of well-**defined**, computer-implementable instructions, typically to solve a class of problems or to perform a computation.



43

Poznámky:

.....

.....

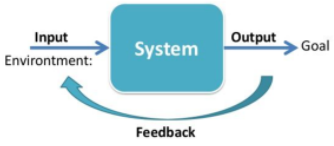
.....

.....

Organizování

Organizování a teorie systémů

- **Teorie chaosu říká, že systém sám hledá svou stabilitu** a po proběhlých nestabilních turbulencích (přechodové jevy) si systém vždy vytvoří sám nějakou stabilní organizaci a řád
  - *Viz. kutálející se tisíci-hran, který se zastaví na nejstabilnější poloze svých hrotů*
  - *Otázka je, zda je pro firmu ideální nechat proběhnout bouři nestabilních jevů než se organizace ustálí*
- **Relevantní Systémové pojmy**
  - *Omezení rozmanitosti systému (variety)*
  - *Struktura systému (získaná, vložená)*
  - *Teorie chaosu a přechodové jevy*
  - *Dynamická rovnováha*



44

Poznámky:

.....

.....

.....

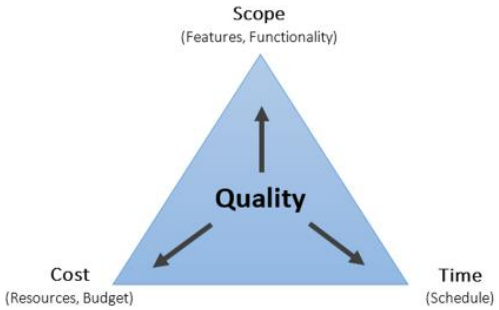
.....

Projektové řízení

Cíle a Kvalita Projektového řízení = Troj-Imperativ

Delivery:

- **On Time**
- **On Budget**
- **On Specification**



45

Poznámky:

.....

.....

.....

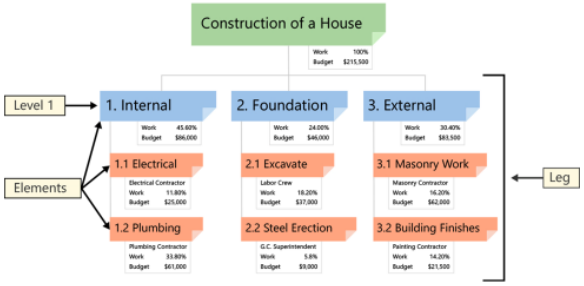
.....

Projektové řízení

WBS – Work Breakdown Structure

A work breakdown structure (**WBS**) is a visual, **hierarchical** and deliverable-oriented deconstruction of a project.

It is a helpful diagram for project managers because it allows them to work **backwards from the final deliverable** of a **project** and **identify all the activities** needed to achieve a successful project.



46

Poznámky:

.....

.....

.....

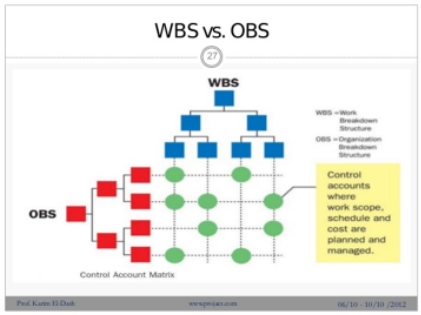
.....

Projektové řízení

OBS – Organization Breakdown Structure

OBS (also known as Organizational Breakdown Structure) is used **to define the responsibilities for project management**, cost reporting, billing, budgeting and project control.

The OBS provides an organizational rather than a task-based perspective of the project.



47

Poznámky:

.....

.....

.....

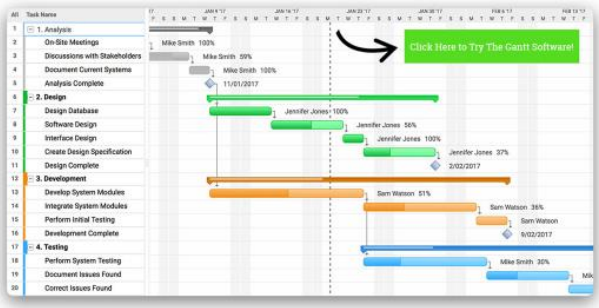
.....

Projektové řízení

Gantt Chart

Ganttův diagram je druh pruhového diagramu pojmenovaný po H. L. Ganttovi, průmyslovém inženýrovi, který byl za první světové války průkopníkem jeho používání.

Ganttův diagram se využívá při řízení projektů pro **grafické znázornění naplánování posloupnosti činností v čase.**



48

Poznámky:

.....

.....

.....

.....

Projektové řízení Rozdíl Agile vs Waterfall

Agile Project Management (Incremental & Iterative Approach vs Waterfall Gantt)

Agile Project Management (Not using => Big Design Upfront as in Waterfall)

Agile project management is an iterative approach to delivering a **project** throughout its life cycle. ... Iterative approaches are frequently used in software development projects to promote velocity and adaptability since the benefit of iteration is that you can adjust as you go along rather than following a linear path.

49

Poznámky:

.....

.....

.....

.....

Projektové řízení

50

Poznámky:

.....

.....

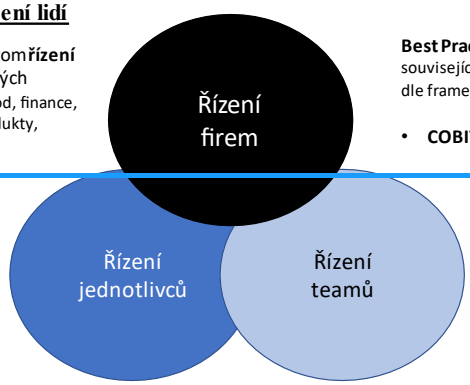
.....

.....

Řízení lidí

Perspektivy řízení lidí

Řízení firem zahrnuje krom **řízení lidí řadu** dalších odborných disciplín řízení jako obchod, finance, technologie, procesy, produkty, marketing ..atd



Best Practice standardy a související metriky, audity, certifikace dle frameworks typu:

- **COBIT, ITIL, ISO …**

Řízení lidí (jednotlivců a teamů) **nelze úplně standardizovat** .

Důraz na soft skills, životní zkušenost a znalosti z oborů jako psychologie, sociologie a další. .

51

Poznámky:

.....

.....

.....

.....

Řízení lidí

Řízení Lidí .. *(Management)*

- **Zadávání úkolů a kontrola**
- *Organizuje a alokuje zdroje*
- *Plánuje a dělá kalkulace*
- *Centralizuje moc a chce mít vše pod kontrolou*
- *Říká **„Já..“** a má averzi ke každému riziku*
- *Chce dělat věci správně (best practice)*
- ***„Korporátní manažer a úředník“***

Vedení lidí … *(Leadership)*

- **Vytváří vize, kterou ostatní následují**
- *Motivuje a deleguje*
- *Vidí cesty a řešení tam kde ostatní nevidí*
- *Deleguje, sdílí a podporuje jednotlivce a teamy*
- *Říká **„My..“** a nevyhýbá se vědomému riziku*
- *Zaměřuje se na správné věci (priority & focus)*
- ***„Podnikatel a leader“***

52

Poznámky:

.....

.....

.....

.....

Řízení lidí

Řízení lidí (Management)

- **Příkazy a kontrola**
  - *„Chain of command“*
- **Řízení výkonu a Cílů**
  - *Performance & Goal management*
- **Motivace & Stimulace**
  - *Cukr a bič „Carrot & Stick“*
- ……a mnoho dalších technik

Řízení lidí a jeho techniky má stále svoje platné místo při řízení jednotlivců, teamů a firem.

53

Poznámky:

.....

.....

.....

.....

Řízení lidí

Principy leadershipu:

A. **Vedení sdílenou vizí**

B. **Zmocňování, Koučování a Delegování „Empowerment & Engagement“**

C. **Vytváření synergie a teamová spolupráce „Enabling Performance“**

D. **Ovlivňovaní a koordinace**

E. **Osobnost a Integrita leadra**

54

Poznámky:

.....

.....

.....

.....

Řízení teamů

Rozdělení teamů dle

A. Diverzity a samostatnosti

B. Lokalizace

C. Typologie členů teamu

D. Pracovní role v teamu

Nástroje pro řízení teamu

A. Socio-mapování, metoda i App.

B. Time is limited, startup

55

Poznámky:

.....

.....

.....

.....

Řízení teamů

Rozdělení teamů dle diverzity

- **Homogenní teamy**
  - Složené s členů s nízkou diverzitou (pohlaví, věk, národnost, země původu, pracovní profil ..atd).
    - *Např. team IT Operation nebo team Finančního kontrolingu v jedné lokální firmě.*
- **Heterogenní teamy**
  - Velká diverzita členů teamu, které zpravidla spojuje společný úkol často řízeného formou projektu.
    - *Např. projekt implementace nového ERP systému nebo GDPR Projekt v rámci EU.*

56

Poznámky:

.....

.....

.....

.....

Řízení teamů

Rozdělení teamů dle samostatnosti

- **Autonomní teamy**
  - Velká míra samostatnosti a odpovědnosti při rozhodování. Často i formální delegace odpovědnosti v rámci Governancenapř. proAgile SW team.
- **Podřízené teamy**
  - V rámci hierarchické struktury napřProgram – Projekt je jasné kdo komu velí a odpovídá, včetně míry samostatnosti.

57

Poznámky:

.....

.....

.....

.....

Řízení teamů

Rozdělení teamů dle lokalizace (1)

- **Lokální teamy**
  - Většinou celý team sedí v rámci jedné firmy a jedné budovy kde se členové teamu pravidelně potkávají a jejich interakce jsou tedy jak formální tak neformální (kafe, oběd, cigárko..)
    - *Tradiční model fungování teamu, který díky globalizaci, nedostatku expertů, covid ..atd. končí.*
- **Vzdálené (Remote) Teams**
  - Geografická distribuce včetně odlišných „Time zones".
    - *Trend v nadnárodních korporacích a globálních projektech kdy se členové teamu často nikdy fyzicky nepotkají a jsou tak odkázáni na prostředky digitální komunikace.*
    - *To vyžaduje velké nároky na vedoucí teamu nastavit funkční governance (..viz team performance) a také soudržnost teamů a jeho socializace je náročnější.*

58

Poznámky:

.....

.....

.....

.....

Risk Management

Risk can be defined as:

An Uncertainty of Outcome

(whether a positive opportunity onegative threat)

59

Poznámky:

.....

.....

.....

.....

Risk Management

1. **Risk Management Process**

60

Poznámky:

.....

.....

.....

.....

(Information) Security Management Domains Overview

Perimeter protection
- **Network** (Vulnerabilities L-WAN, DDos, NBA ...)
- **Physical** (Assets monitoring, DCs, ...)
- **End Point Equipment** (AV at PC, Mobile...)
- **Complex systems** (Penetration testing, ...)

Data & Privacy protection
- **Identity mgmt.** (..., ...)
- **Data privacy & security** (DLPs, ...)
- **Ethics by Design** (....)
- **TBD** (AVAST inspiration, ...)

Security Consulting
- Risk Analysis
- Security Audits
- IT Governance consulting

Processes protection
- **ISO Standards** (27 00x, 20 00x, 9 00x, ...)
- **COBIT 5** & **ITIL 4.0** & **PMI & Prince 2** (....)
- **Compliance proj.** (GDPR, PCI DSS, Mifid, ...)
- **Other** Frameworks (Industry Specifics, ...)

Application protection
- **Applications** (Code review, ...)
- **Databases** (Encryption, Role & Rights, ...)
- **Infrastructure** (Kubernetes, Docker .)
- **APIs & IF** (Public, Private API, ...)

61

Poznámky:

.....

.....

.....

.....

Security Management

Security Consulting
- Risk Analysis
- Security Audits
- IT Governance consulting

62

Poznámky:

.....

.....

.....

.....

Security Consulting

Risk management

- **Risk mgmt. process**
  - Identify, Asses, Evaluate, Control & Monitor
- **Risk matrix**
  - Probability vs Impact
- **Mitigation Plan**
  - Implement Measures & Act proactively
  - Minimize Risk impact
  - Maximize Opportunities

Security Audit

Types of Audit

- Assurance x Assesment x Audit
- External, Internal & special area audits (Financial, Information Security...etc)

Standards and Authorities

- Sarbanes-Oxley Act (SOX) of 2002
- ISO 27 00x, ISACA & COBIT, ...etc.
- Certified Auditors

Audit Process

- **Objectives** must be defined first.
- **Plannning** procedure is essential.
- **Report** is Summary & Detail per Obj. areas

IT Governance consulting

- *See previous COBIT lectures.*

63

Poznámky:

.....

.....

.....

.....

Definice Etiky (1)

Etika

Je disciplínou praktické filosofie a hledá odpověď na základní otázku lidské existence a rozhodování v každodenních situacích tedy:

„Jak správně žít?“

„How we ought to live.“

„Socrates“

64

Poznámky:

.....

.....

.....

.....

Definice Etiky (3)

Pohledy na různé úrovně etiky:

Jan Sokol a jeho tři pohledy:

1. **Individuální morálka**
   1. *Pravidla a hodnoty podle, kterých se jako jednotlivec chovám (Desatero, Zlaté pravidlo..)*
2. **Společenský mrav**
   1. *Zvyk dané společnosti (rodina, vesnice...stát), ale pozor na překročení hranic „okresu“ a střet kultur*
3. **Etika jako hledání nejlepšího**
   1. *Tedy neustálé kladení otázky „Jak správně žít“ v různých kontextech*

65

Poznámky:

.....

.....

.....

.....

Definice Etiky (9)

Aplikovaná etika

- **je nutné jí zkoumat ve vzájemném vztahu ke konkrétnímu oboru lidské činnosti.**
- Vyjadřuje se ke konkrétním, praktickým otázkám, které se týkají etických rozhodnutí.

Podnikatelská etika (obecně typ profesní etiky)

- řeší konflikt mezi vlastním sebe-zájmem a zájmy ostatních lidí, konflikt odedávna spojovaný s obchodní činností. Je to však nová disciplína, která hledá teoretické koncepty a modely chování firem.
- V podnikatelské etice jde o reflexi etických principů do veškerých podnikatelských činností zahrnujících individuální i korporativní hodnoty.
  - ***Podnikatelská etika je reflexí své doby.*** *(viz. divoká privatizace v ČR nebo rozdíl podnikání v Rusku a USA)*

66

Poznámky:

.....

.....

.....

.....

Firemní kultura (8)

Změna firemní kultury

Jak udělat z neúspěšné firmy úspěšnou?

67

Poznámky:

.....

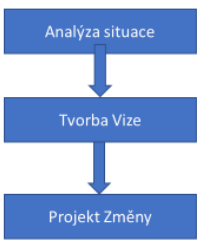
.....

.....

.....

Firemní kultura (9)

Změna firemní kultury



Čas změny: 2-3 roky je úspěch

Aktéři změny:

- Iniciátoři & Leader & Reprezentanti změny
- Podporovatelé, Odpůrci a Neutrální zaměstnanci

Nástroje změny:

- Vize a Projekt změny firemní kultury
- Personální a Organizační změny
- Vzdělávání a výcvik
- Změny v odměňování a přidělování zdrojů
- Technologické změny
- Tvorba pracovního prostředí a související artefakty nové kultury

68

Poznámky:

.....

.....

.....

.....

Dokumenty a Normy

Firemní dokumenty a jejich příklady:

- Smlouvy
- Zápisy z jednání
- Organizační normy
- Prodejní a reklamní dokumentace
- Projektová dokumentace ..a další

Zásadní členění firemní dokumentace je:

Řízená vs **Neřízená**

69

Poznámky:

.....

.....

.....

.....

Dokumenty a Benefity

Přínosy řízené dokumentace:

- **Pořádek** – *veškeré důležité dokumenty na jednom místě a odstraňuje se nejistota při řízení firmy i časové prodlevy*
- **Dostupnost** – *dokumenty snadno vyhledatelné i dostupné kdykoliv a odkudkoliv*
- ***Spolehlivost a Kvalita Informací*** – *veškerou tvorbu, evidenci, připomínkování, ověřování, schvalování, zveřejňování a další úkony řídí nastavený systém (ISO 9000 pravidla … SW)*
- ***Bezpečnost*** – *kdo a jaké úkony smí s dokumentem provádět je stanoveno předpisem organizace a následně sledováno (logs)*
- ***Archivace*** – *dokumenty jsou řízeně uschovány pro další použití*

70

Poznámky:

.....

.....

.....

.....

Dokumenty a SW nástroje (9)

Další systémy a formy ECM

- **Document Imaging** (DI) – skenování dokumentů,
- **Document Management** (DMS) – správa dokumentů v elektronické podobě,
- **Web Content Management** (WCM) – správa obsahu webových prezentací a aplikací,
- **Digital Asset Management** (DAM) – správa multimediálních dat; jedná se o úzce zaměřenou oblast ECM, která podporuje multimediální data – fotografie, audio nebo video záznamy,
- **Records Management** (RM) – správa dokumentů, jejichž obsah již nelze měnit, a přesto musí být archivovány vzhledem ke své platnosti – například podepsané smlouvy, přijaté faktury, účetní uzávěrky; jedná se více méně o elektronický archiv, který kontroluje skartační a archivační lhůty dokumentů,
- **Team Collaboration** (TCM) – slouží k podpoře rozhodovacích procesů

71

Poznámky:

.....

.....

.....

.....

Dokumenty a SW nástroje (ECM 1)

Enterprise Content Management (ECM)

- Je podnikový informační systém, který se zabývá správou podnikových informací.
- Obsahem jsou nejen elektronické a papírové dokumenty, ale řízení a správa veškerého informačního obsahu, který společnost vytváří a využívá.

Podniková data:

- **Strukturovaná data** – data uložená v databázích, ve struktuře, která umožňuje vyhledávání
- **Nestrukturovaná data** – dokumenty, emaily, smlouvy, nabídky
- *Všechny typy elektronických dat* - fotografie, videa, audio, web, IoT…
- *Součástí práce s podnikovými daty je proces digitalizace* (dokumentů, procesů…)

ECM je nadřazený název pro další dílčí systémy správy inf. obsahu (DMS, WCM..)

72

Poznámky:

……

……

……

……

Dokumenty a SW nástroje (ECM 2)

Cíle ECM

- Zajištění dostupnosti informací
- Zvýšení informační bezpečnosti,
- Snížení chybovosti
- a **úspory** *(nárůst rychlosti, přesnosti a kvality zpracování).*

73

Poznámky:

……

……

……

……

Dokumenty a SW nástroje (W-Flow)

Digitální Work-Flow

- **Automatizace** jednotlivých částí nebo celého **podnikového procesu**, během něhož jsou **dokumenty** (informace) nebo **úkoly předávány od jednoho účastníka procesu ke druhému podle přesně definovaných pravidel.**

- **Cílem je efektivně** *(levněji, rychleji, paralelizací, asynchronní komunikací…)* **přispět k naplnění** cílů procesu a celkových **cílů podniku**.

Digitalizace Work-Flow je základ „Digital Transformation“

74

Poznámky:

……

……

……

……

Normy (1)

Globální kaskáda impulsů pro vznik norem:

- *Legislativa – Oborové standardy – Firemní standardy*

75

Poznámky:

.....

.....

.....

.....

Normy (2)

Firemní kaskáda pro vznik norem:

- *Compliance*
- *Best Practice*
- *Quality management*

76

Poznámky:

.....

.....

.....

.....

Normy (3)

Norma o normě

- **Základem normotvorného procesu je základní norma o tom, jak psát normy**
- Vytvoří se v organizace jako první norma a ostatní se pak píší podle tohoto vzoru
- **Stanoví se struktura obsahu**
  - *Typ normy, Pořadí kapitol, záhlavím zápatí, schvalovací schéma a podpisy..*
- **Stanoví se forma**
  - *Velikost a druh písma, číslo kapitol, odstavců a nadpisů, formáty obrázků, výkresů a příloh..*

77

Poznámky:

.....

.....

.....

.....

Normy (4)

Význam norem v podniku

- **Vytváří se jimi „normativní model" organizace tedy pravidla jak má správně fungovat aby plnila své cíle**
- V souladu s normou se tvoří a upravuje systém řízení organizace, viz. principy EGIT.
- Nově schválená norma se začlení do soustavy již existujících norem
- **Nastavit Normativní chování je efektivní, ale pozor** na balanc **Formálnosti vs Kreativity** (Inovace).
- Normovat (Regulovat) je třeba jen to co je nutné, ideálně nutné minimum
  - *viz. dopad na inovace a kreativitu*
  - *viz. princip přiměřenosti a proporcionality (střet více hodnot či práv, řeším v kontextu a dávám přednost důležitějšímu)*
  - *Obecněji otázka řízení společnosti a (Svoboda vs Rovnost a Pravice vs Levice)*

78

Poznámky:

.....

.....

.....

.....

Normy (5)

Druhy norem

- **Směrnice**
- **Nařízení**
- **Rozhodnutí ředitele**
- **Opatření**
- **Normativní směrnice**
- **Řád**
- **....**

Hierarchie norem

- **Nastavena organizaci v základní normě**
- Přehlednost zpravidla podpořena systémem značení a číslování norem
  - *..např.* ***Sm-Org-2021-153-28***
- **Externí právní normy (ČR, EU) jsou vždy nadřazeny**

79

Poznámky:

.....

.....

.....

.....

Normy (6)

Kategorizace vnitropodnikových norem

- **Právní**
- **Technické**
- **Ekonomicko-Provozní (THP)**
- **Organizační**
- **Řídící**
- Ostatní

Příklady vnitropodnikových norem

- **Stanovení normativního procesu**
- **Organizační a podpisový řád**
- Stanovení účetních standardů
- Systém řízení rizik společnosti
- Provozní zajištění společnosti
- Krizový plán a BCM/DR
- Nastavení systému hodnocení a odměňování
- A další.

Poznámky:

.....

.....

.....

.....

Poznámky:

.....

.....

.....

.....

Závěr

..To be continued...

36

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

Informační bezpečnost / bezpečnost informací / kryptografie

Repetitorium pro přijímací zkoušky

Luboš Pavlíček
Vysoká škola ekonomická v Praze

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Bezpečnost informací

Bezpečnost informací (*informační bezpečnost, information security*) představuje ochranu informací ve všech jejich formách a po celý jejich životní cyklus

Důvěrnost (confidentiality)
- informace by měli být přístupné jen tomu, kdo je oprávněn

Integrita (integrity)
- zabránit neautorizovaným změnám systému a informací

Dostupnost (availability)
- nenarušit dostupnost systému a služeb

tzv. bezpečnostní triáda (CIA triad)

2

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Bezpečnost informací

Důvěrnost (confidentiality)
- ochrana před neautorizovaným přístupem, užitím či vyzrazením
- ochrana dat umístěných v systému, při přenosu či při zpracování
- metody: fyzická bezpečnost (dveře, ochranka, kamery, ...), šifrování, autentizace, autorizace (přístupová práva)

Integrita (integrity)
- detekce nežádoucích změn při uložení, při přenosu, při zpracování
- metody: digitální podpisy, haše, auditování operací, odolnost k chybám uživatele,

Dostupnost (availability)
- zajištění dostupnosti systému, služeb a informací pro uživatele
- akceptovatelná úroveň výkonnosti,
- prevence ztráty a zničení
- metody: redundance uložení, zpracování či přístupových tras; zálohování a obnova dat; plány obnovy; aktualizace a záplatování; řízení prostředí (elektřina, chlazení, požární čidla, ...)

3

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Bezpečnost informací vs Kryptografie

Cíle kryptografie (*cryptography*):

- **důvěrnost** (confidentiality) – též bezpečnost
- **integrita dat** (data integrity) – též celistvost dat
- **autentizace** (authentication) – prokázání totožnosti (ověření subjektu), prokázání původu dat (vlastnictví)
- **nepopiratelnost**, neodmítnutelnost (non-repudiation)

Cíle bezpečnosti informací:

- **důvěrnost**
- **integrita**
- **dostupnost**

4

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Bezpečnost informací vs Kybernetická bezpečnost

Kybernetická bezpečnost (*cybersecurity*)

- souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru

Bezpečnost informací a kybernetická bezpečnost

- překrývají se, často se používají jako synonyma
- bezpečnost informací chrání i analogové informace, chrání i před jinými hrozbami (požár, krádež zařízení, ...)
- kybernetická bezpečnost může chránit i jiná aktiva než informace (soukromí, zařízení (semafory), ...)

5

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Pojem kryptografie

- **Kryptografie** se zabývá **matematickými metodami** se vztahem k takovým prvkům **informační bezpečnosti** jako je **důvěrnost zprávy, integrita dat, autentizace entit a původu dat.**
- **Kryptoanalýza** – analýza odolnosti kryptografických systémů, hledání metod k proniknutí do těchto systémů.
- **Kryptografická primitiva**
  - algoritmy se základními kryptografickými vlastnostmi

6

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Cíle kryptografie

- **důvěrnost** (confidentiality) – též bezpečnost
- **integrita dat** (data integrity) – též celistvost dat
- **autentizace** (authentication) – prokázání totožnosti (ověření subjektu), prokázání původu dat (vlastnictví),
- **nepopiratelnost**, neodmítnutelnost (non-repudiation)
  - *Alice podepíše směnku a po měsíci prohlásí, že to není její podpis*
  - částečně sociálně právní cíl,
  - otázky:
    - Jaké je jméno na směnce? identifikace
    - Patří Alice (osoba) k tomu jménu? autentizace
    - Měla právo směnku podepsat? autorizace
    - Není směnka zfalšovaná? integrita
    - Je směnka k dispozici? dostupnost

7

Poznámky:

.....

.....

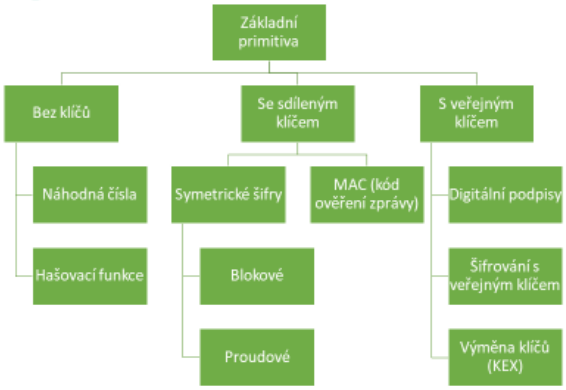
.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Kryptografická primitiva



8

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Entropie, bit, síla zabezpečení

Entropie měří množství informace ve zprávě, měří se pomocí $\log_2$ a udává se v bitech,

PIN ze čtyř náhodně vybraných číslic má entropii $\log_2 10^4 = 13.29$ *bitů*

Symetrická šifra AES, délka klíče 128 bitů. Pokud se při šifrování zvolí náhodný klíč (*viz generátory náhodných čísel*), tak entropie klíče je 128 bitů.

Síla zabezpečení (security strength)

počet operací, které jsou nutné na prolomení kryptografického algoritmu/systému. Měří se pomocí $\log_2$ a udává se v bitech,

9

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Entropie klíče vs síla zabezpečení

Je síla zabezpečení stejná jako entropie klíče?

Máte soubor zašifrovaný pomocí AES-128, je síla zabezpečení 128 bitů?

- **slabiny v algoritmu** – současné odhady síly zabezpečení pro AES-128 jsou 126.1 bitů,
- **technologický pokrok** – kvantový algoritmus snižuje sílu zabezpečení na polovinu, tj. na ~64 bitů,
- **klíč odvozen ze hesla? –** pokud ano, jakou entropii (sílu zabezpečení) má heslo?
- **klíč náhodně vygenerován?** – jak kvalitní je použitý generátor?
- **postranní kanály** – nezůstala na disku nešifrovaná verze?, není někde uložen klíč?, nebyl podvržen generátor náhodných čísel?

10

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Hašovací (hash) funkce

- **Hašovací funkce**

  Libovolný vstupní řetězec převede na **otisk** pevné délky

  $$\boldsymbol{h} = hash(\boldsymbol{x})$$

- **Užití v kryptografii**
  - ověřování hesla (hašování hesel)
  - ověření integrity zpráv a souborů
  - generování a ověření digitálního podpisu
  - důkaz práce (Proof of Work, bitcoin)
  - identifikátor souboru nebo dat (git, Mercurial)

11

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Kryptografické hašovací funkce

Kryptografická hašovací funkce

1) pro daný haš $\boldsymbol{h}$ je prakticky nemožné spočítat $\boldsymbol{x}$ takové, že $hash(\boldsymbol{x}) = \boldsymbol{h}$.
2) pro daný vstup $\boldsymbol{x}$ je nemožné spočítat takové $\boldsymbol{y}$, že $\boldsymbol{x} \neq \boldsymbol{y}$ a současně $hash(\boldsymbol{x}) = hash(\boldsymbol{y})$
3) je nemožné najít **dvojici libovolných** vstupů $(\boldsymbol{x}, \boldsymbol{y})$, pro které platí $\boldsymbol{x} \neq \boldsymbol{y}$ a současně $hash(\boldsymbol{x}) = hash(\boldsymbol{y})$

- pro ukládání hesel je potřeba odolnost vůči 1)
- pro zajištění integrity je potřeba odolnost vůči 2)
- pro vytváření a ověření podpisů je potřeba odolnost vůči
  - odhalení, k čemu se subjekt zavázal 1)
  - vytváření falešných podpisů 3)

12

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Útoky na hašovací funkce

- **Nalezení prvního vzoru (pre-image resistence)**
  - síla zabezpečení ideálně odpovídá délce otisku
  - SHA1 má otisk 160 bitů, síla zabezpečení ideálně 160, slabiny v algoritmu ➔ 150 bitů,
- **Nalezení druhého vzoru (second pre-image resistence)**
  - síla zabezpečení je minimálně stejná jako u nalezení kolizí, ideálně jako nalezení prvního vzoru,
  - SHA1 reálně – 105 až 110 bitů,
- **Nalezení kolize**
  - narozeninový paradox,
  - síla zabezpečení je ideálně polovina délky otisku,
  - SHA1 – ideálně 80 bitů, chyby v algoritmu ➔ 61 bitů (sha-mbles)
  - kolizní útok se zvoleným prefixem ➔ 63 bitů

13

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Symetrická šifra

- **Pro šifrování i dešifrování se používá stejný klíč**
  - tajný klíč, symetrický klíč, klíč sezení (session key)
- Požadavky:
  - **Bezpečný šifrovací algoritmus**. Informace o použitém algoritmu je veřejná.
  - Tajný klíč je znám pouze odesílateli a příjemci (oprávněným osobám). To vyžaduje tajný kanál (**secure channel**) pro distribuci klíče.
- Základní typy symetrických šifer:
  - **Blokové šifry** – rozdělení otevřeného textu na bloky,
  - **Proudové šifry** – průběžné šifrování

14

Poznámky:

.....

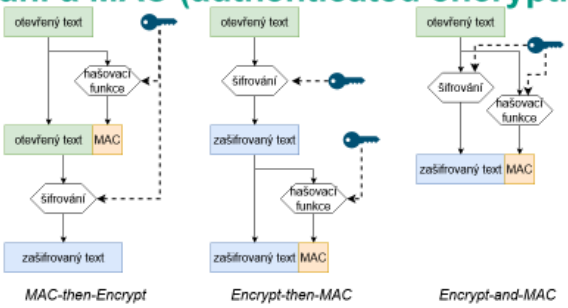
.....

.....

.....

fis.vse.cz fisvse

Šifrování a MAC (authenticated encryption)



MAC-then-Encrypt	SSL/TLS < 1.3	*lze zneužít k DOS útokům*
Encrypt-then-MAC	IPsec, SSH	*jediná v NÚKIB,*
Encrypt-and-MAC	SSH	

15

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Symetrická šifra - AEAD, GCM

AEAD (Authenticated encryption with associated data)

- cílem je současně zašifrovat a spočítat MAC,
- bezpečnější než kombinace šifra+MAC

- GCM (Galois/Counter) mód blokových šifer
  - Podporován v TLS 1.3
- CCM mód blokových šifer
  - v IPsec, v TLS 1.2
- POLY1305 pro ChaCha proudovou šifru
  - v TLS 1.2, 1.3

V TLS 1.3 mohou být pouze AEAD šifry

16

Poznámky:

.....

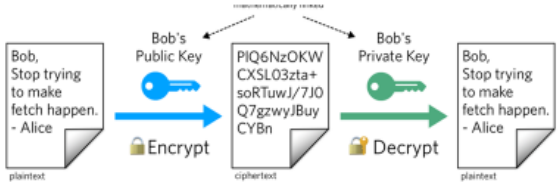
.....

.....

.....

fis.vse.cz fisvse

Asymetrická kryptografie



analogie:

- poštovní schránka na klíč (šifrování):
  - kdokoliv může vložit dopis, pouze vlastník klíče (Alice) může schránku otevřít,
- královská pečeť (podepisování):
  - kdokoliv pozná na dokumentu pečeť od krále, ale pouze král ji může na dokument otisknout

17

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Matematické problémy asymetr. kryptog.

Základem jsou „jednosměrné“ funkce, matematicky obtížné problémy:

- výpočet $y = f(x)$ je snadný a rychlý
- výpočet $x = f^{-1}(y)$ je výpočetně velmi náročný

Tři základní skupiny:

- rozložení velkého čísla na součin prvočísel – faktorizace (RSA)
- diskrétní logaritmus (Diffie-Hellman, Elgamal, DSA)
- eliptické křivky EC (ECDH, ECDSA, ECIES, Ed25519, Curve25519)

Všechny tři případy jsou málo odolné vůči kvantovým počítačům, NIST vyhlásil soutěž na kvantově odolné asymetrické algoritmy

18

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Asymetrická kryptografie - užití

Šifrování

- vyřešena distribuce klíčů (skoro) – veřejný klíč může mít kdokoliv, dešifrovat může pouze vlastník privátního klíče,
- pomalé, přibližně 1000x proti symetrickému šifrování ➔ hybridní šifrování

Podepisování (digitální podpis, digital signature):

- podepsat může pouze vlastník privátního klíče, ověřit podpis může kdokoliv (veřejný klíč je veřejný)
- nelze zfalšovat podpis (neodmítnutelnost) – skoro,
- lze použít pro autentizaci (přihlašování)

Výměna klíčů, domlouvání klíčů (key exchange)

- Alice a Bod si mohou domluvit sdílené tajemství na nezabezpečeném kanálu,

19

Poznámky:

.....

.....

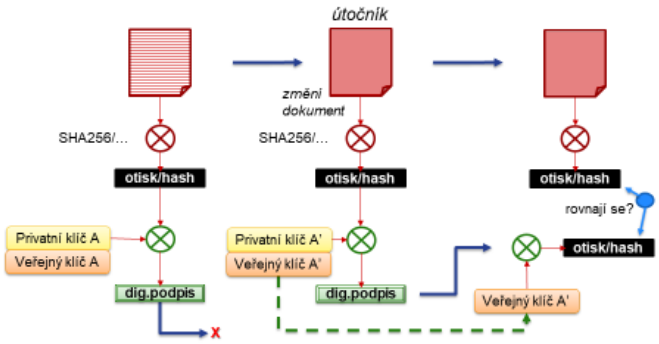
.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Útok na digitální podpis



20

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Certifikát

Certifikát je datová struktura která obsahuje:

- identifikační údaje,
- platnost certifikátu,
- veřejný klíč,
- rozšiřující údaje,
- digitální podpis těchto údajů od certifikační autority.

Version
Serial Number
Issuer Name
Validity Period
Subject Name
Public Key Information
Extensions
Signature

21

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Důvěryhodná certifikační autority (CA)

- **Důvěra** – důvěřujeme CA, že nevydá certifikát se jménem Alice např. Mallorymu,

Otázky:

- Kterým CA důvěřujete?
- Potvrzovali jste někdy důvěru nějaké ca?
- Jak zjistíte postup konkrétní ca při ověřování žadatelů o certifikáty?
- Existují úrovně kvality ověření?
- Může být stejná ca důvěryhodná pro více účelů certifikátu (pro servery, pro e-mail, pro podepisování dokumentů, …)?

22

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fisvse

eIDAS

eIDAS – nařízení EU 910/2014 o elektronické identifikaci a důvěryhodných službách

- e-Signature
  - elektronické podpisy
  - elektronické pečeti
  - časová razítka
- e-ID (eldentification)
- e-Delivery
- *webové certifikáty ?*

23

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Elektronické podpisy

Kvalifikovaný certifikát – vydala kvalifikovaná certifikační autorita (CA které důvěřuje stát/EU), obsah musí být pravdivý (garantuje stát)

Kvalifikovaný prostředek – nelze z něho získat soukromý klíč, musí mít EU certifikát

druh el. podpisu	kvalita certifikátu	uložení privátního klíče
kvalifikovaný el. podpis	kvalifikovaný certifikát	kvalifikovaný prostředek
uznávaný el. podpis	kvalifikovaný certifikát	žádný požadavek
zaručený el. podpis	žádný požadavek	žádný požadavek

Pozor – je to vztah z hlediska komunikace osoba–stát

24

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Elektronické pečeti

Elektronické pečeti (Electronic Seals)

- shodují se s el. podpisy po technické stránce
- kvalifikovaná, uznávaná, elektronická, „prostá“
- mají „jiné“ certifikáty
- mají jiné právní důsledky

Podpisy	Pečeti
pouze fyzické osoby	pouze právnické osoby
podpis je projevem vůle fyzické osoby	pečeť je vyjádřením původu
lze podepsat i cizí dokument	pečetit lze pouze vlastní dokument
podepisuje se obvykle „ručně“	pečetí se strojově
kvalifikované prostředky jsou levné (stovky Kč)	kvalifikovaná prostředky jsou drahé

25

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Časová razítka (časové značky)

Popis problému:

Alice pošle Bobovi pojistnou smlouvu. Bob s podpisem čeká, vznikne pojistná událost. Bob vrátí na počítači čas zpět, podepíše digitálně smlouvu a předá Alici. A chce vyplatit pojistné plnění – *tvrdí, že podepsal před pojistnou událostí*.

Otázka – jak garantovat čas podpisu dokumentu?

Autorita pro vydávání časových značek (Time Stamp Authority, TSA),

- k otisku přidá časovou značku, pořadové číslo a celek digitálně podepíše.

26

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Identifikace, autentizace, autorizace, odpovědnost

Identifikace (identification)

- Akt nebo proces, během kterého entita předloží systému nějaký identifikátor, na jehož základě systém může rozeznat entitu a odlišit ji od jiných entit.

Autentizace / autentizace identity (authentication)

- Provedení testů, umožňujících systému rozpoznání a potvrzení entity.

Autorizace (authorization)

- Udělení práv, které zahrnuje udělení přístupu na základě přístupových práv. Proces udělení práv subjektu pro vykonávání určených aktivit v systému.

Accountability (odpovědnost), **Accounting**

- Odpovědnost entity za její činnosti a rozhodnutí. **Auditování** je sledování činnosti entity a vytváření záznamů o jeho činnosti. Auditování zajišťuje odpovědnost.

27

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Fyzická a elektronická identita

- Fyzická osoba existuje jen 1x ➔ **fyzická identita** je jen jedna
- Údaje o osobě mohou být v různých elektronických evidencích, databázích
  - v evidenci jsou dílčí údaje o osobě (jméno, příjmení, datum narození, bydliště, …)
    ➔ vytvářejí **elektronickou (digitální) identitu** příslušné osoby
- K jedné fyzické identitě je více elektronických identit
- Elektronická identita je právní i technický pojem,
- **Uživatelský účet**
  - souvisí s přihlašováním, s možností využívat konkrétní službu

28

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Autentizace – faktory

- Něco co **vím**, co si pamatuji (např. heslo)
  - typicky heslo či PIN,
  - nakreslení gesta,
  - obrázkové heslo (Windows)
  - otázky na obnovu hesla („Jméno matky za svobodna")
- Něco co **mám**,
  - platební karta,
  - mobilní telefon,
  - osobní doklady,
  - ***lze zcizit***
- Něco co **jsem** (biometrie),
  - otisk prstu, obličej, sken sítnice, …
  - *nelze změnit při prozrazení,*
  - *lze udělat kopii,*
  - **lze používat pouze jako druhý faktor !!!**

co s následujícími omezeními, jsou to faktory?
- CAPTCHA
- omezení přihlášení na lokalitu,
- omezení přihlášení časem,

29

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Přihlašování heslem

- nejčastější způsob autentizace,
- nejjednodušší na implementaci,
- jednoduchý a známý pro uživatele,
- nejméně bezpečný,

30

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Hesla - pravidla National Cyber Security Centre (UK)

1. **Omezit používání hesel**
   - heslo je slabý verifikátor
   - single sign on, používání klíčů či hw zařízení,
   - podporovat použití vícefaktorové autentizace
2. **Chránit hesla uživatelů**
   - bezpečné ukládání hesel (PBKDF, hašovací funkce Argon či Bcrypt)
   - bezpečný přenos hesel (HTTPS)
   - speciální požadavky na autentizaci administrátorů,
   - změnit defaultní hesla
3. **Školit uživatele**
   - rizika použití hesla na více místech
   - různé účty jsou různě cenné (prioritizace)
   - správce hesel

National Cyber Security Centre

31

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Hesla - pravidla National Cyber Security Centre (UK)

4. **Technická opatření**
   - omezit počet neúspěšných pokusů o přihlášení
   - monitorovat přihlašování – hledat anomálie
5. **Pomáhat uživatelům vytvářet hesla**
   - nevyžadovat zbytečné nároky na hesla,
   - neumožnit slabá hesla pomocí slovníků slabých hesel (zxcvbn, haveibeenpwned)
   - podporovat generovaná hesla ze správců hesel
   - neomezovat uživatele při vytváření hesel (znakové sady, max délka)
6. **Nepřetěžovat uživatele hesly**
   - podporovat ukládání do správců hesel
   - hesla expirovat v případě bezpečnostní události, ne preventivně
   - podporovat delegování práv a ne sdílení hesel

National Cyber Security Centre

32

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Vícefaktorová autentizace

- Dvoufaktorová autentizace (two factor authentication, 2FA)
  - použití dvou různých faktorů
  - např. privátní klíč chráněný heslem,
- Dvoufázová/dvoukroková autentizace (two step verification 2SV)
  - postupně,
  - např. heslo plus opsání kódu z mobilu (OTP, SMS)
- Práva v závislosti na úrovni autentizace
  - pouze heslem – jen číst,
  - 2FA/2SV – možnost i zapisovat,
- V praxi nemá smysl rozlišovat pojmy 2FA a 2SV
- Vytvořte model útoků na autentizaci a posuzujte jednotlivá rizika

Two step verification or two factor authentication?

33

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY fis.vse.cz fisvse

Single Sign-On (SSO)

- Oddělení aplikace od autentizace uživatelů
- Přístup s jedním přihlášením na více nezávislých, ale souvisejících systémů

- Výhody SSO:
  - **oddělení provozu aplikace (webu) od správy autentizace**
  - **úspěšný útok na aplikaci neznamená prozrazení hesel uživatelů**
  - **uživatel si nemusí pamatovat více jmen/hesel**
  - úspora času při zadávání přihlašovacích údajů
  - menší zatížení podpory na problémy s hesly
  - podpora cloudových služeb v některých řešeních
  - podpora autorizace API v některých řešeních

34

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY fis.vse.cz fisvse

Základní typy SSO

- „webové“ – přes cookies
  - LemonLDAP - https://lemonldap-ng.org
  - CAS (Central Authentication Services) - https://en.wikipedia.org/wiki/Central_Authentication_Service

  oba nyní mají prvky z federovaných autentizačních protokolů

- Federované autentizační protokoly
  - SAML (Security Assertion Markup Language)
  - OpenID Connect

- Kerberos – lokální sítě
  - unix,
  - active directory

35

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY fis.vse.cz fisvse

Historie standardů pro SSO

protokol	rok	popis
SAML 2.0	2002-2005	komplexní protokol pro autentizaci, řeší různé možné situace ve firemním prostředí a používání cloudových služeb, není vhodný pro samostatné zákazníky, neřeší autorizaci API,
WS-Fed(eration)	2009	součást Web Services standardů (WS-*), zjednodušená verze SAML 2.0
OpenID	2005	řešení pro autentizaci zákazníků, OpenID 2.0 v roce 2006, od 2007 podporoval AOL, od 2008 Yahoo či Google, v současnosti se téměř nepoužívá
OAuth 1.0	2007	API autorizace,
OAuth 2.0	2012	API autorizace, používá Google, Facebook, ...
OpenID Connect (OIDC)	2014	autentizace postavená nad OAuth 2.0

SP potřebuje: ***identifikátor uživatele*** + ***atributy o uživateli*** (např. e-mailovou adresu)

36

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY fis.vse.cz fisvse

eIDAS a autentizace

- Cíl – uznávání autentizace mezi státy EU
- Úroveň záruky (míra spolehlivosti totožnosti určité osoby):
  - nízká
  - značná
  - vysoká
- Úroveň záruky je pro:
  - vydání elektronické identity (registraci) – získání atributů, předání verifikátoru
  - použití verifikátoru (autentizaci)
  - revokaci a vydání nového verifikátoru
- Každá služba musí deklarovat, jakou úroveň záruky požaduje
  - je to pro přihlášení ke službě

37

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY fis.vse.cz fisvse

eIDAS – vydávání (enrolment)

- **Nízká**
  - existence důkazu deklarované totožnosti uznávaný státem,
  - důkaz je pravý a jeví se platným,
- **Značná**
  - navíc zohledněno riziko ztráty, zcizení či vypršení platnosti,
- **Vysoká**
  - navíc důkaz opatřený fotografií či biometrickými údaji a provede se kontrola fyzických vlastností osoby
  - nebo stejné postupy, jako při vydávání dokladů uznávaných státem s fotografií či biometrickými údaji

uživatel musí být seznámen s podmínkami a s bezpečnostními opatřeními,
shromáždit údaje o prokázání a ověření totožnosti,
pravidla pro identifikaci právnických osob,

38

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY fis.vse.cz fisvse

eIDAS správa prostředků pro el. identifikaci

úroveň	vlastnosti, forma	doručení	obnovení, výměna
nízká	jeden faktor	může dostat určená osoba	stejná záruka či stejné ověření
značná	dva faktory	může dostat pouze vlastník	stejná záruka či stejné ověření
vysoká	nelze vytvořit duplikát	prokázat, že dostal pouze vlastník	stejná záruka či stejné ověření,

- dále:
  - musí umožnit pozastavení či zrušení autentizace,
  - zabránit neoprávněnému pozastavení/zrušení autentizace,
  - při autentizaci omezit možnosti hádání, odposlechu či manipulace ze strany útočníka,
  - vedení záznamů,
  - technické kontroly, SŘBI

39

Poznámky:

.....

.....

.....

.....

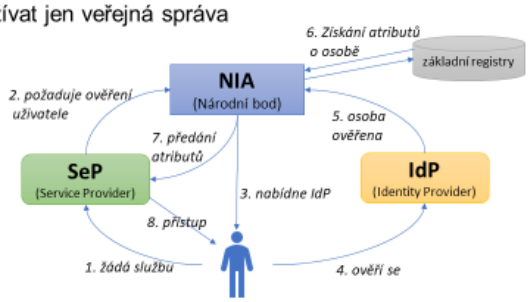
VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

NIA Národní bod pro identifikace a autentizaci

- v ČR nepřímý model
  - IdP neví, k jaké službě se uživatel hlásí
  - SeP neví, jak se uživatel autentizoval
- NIA může používat jen veřejná správa

identita.cz
KLÍČ K ELEKTRONICKÝM SLUŽBÁM



40

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Penetrační testování

- Plánování a příprava
  - výměna kontaktů, ujasnění postupů a zaměření testů, souhlas zákazníka s konkrétními postupy
- Ohodnocení
  1) sběr informací
  2) mapování sítě
  3) identifikace bezpečnostních slabin
  4) průnik do infrastruktury
  5) získání přístupu a vystupňování přístupových oprávnění
  6) zajištění stabilního přístup
  7) zahlazení stop

stejný průběh má cílený útok

- Reportování

41

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

OWASP Top Ten (2021)

1. Chybně nastavená přístupová práva
2. Chyby v šifrování (kryptografie)
3. Injection (podvržení kódu) – SQL, ...
4. Chybný návrh (design)
5. Chybná konfigurace
6. Staré zranitelné komponenty
7. Chyby v identifikaci a autentizaci
8. Chyby v aktualizacích
9. Chyby v logování a monitorování
10. Útoky na servery

https://owasp.org/Top10/

42

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Firewall

Blokuje nebo povoluje navazované komunikace na základě předdefinovaných nebo dynamických pravidel a politik. Chrání zařízení, jež jsou zapojena za ním, před různými typy útoků.

Techniky blokování:

- **drop** – paket se zahodí,
- **reject** – pošle se ICMP zpráva o nedostupnosti služby/protokolu
- **tcp reset** – pošle se TCP RST

někdy se mezi firewally řadí proxy servery (aplikační brány), ale ty mají odlišné síťové chování

43

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Firewall – rozdělení

Dle schopností:

- **bezstavový firewall** (první generace, filtrování paketů)
- **stavový firewall** (druhá generace)
- **aplikační firewall** (třetí generace, aplikační vrstva OSI modelu)
- **firewally nové generace** (next generation firewall)

Dle umístění:

- **na hranici sítě,**
- **mezi subnety**,
- **v operačním systému**,
- **v aplikaci**,

kam zařadíte **web application firewall**?

44

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Firewall na hranici sítě (na perimetru)

Ochrana vnitřní sítě před útoky ze „zlého" internetu,

Problém jak definovat hranici sítě:

- je Office 365 součást školní sítě?
- studenti jiných škol připojení na eduroam jsou uvnitř či vně?
- zařízení studentů VŠE (koleje, eduroam) – jsou uvnitř či vně?
- učitelé mají administrátorská práva na notebooku – mají být uvnitř či vně?
- měli by mít všichni uvnitř přístup ke kamerám či k IP telefonům?

VŠE: téměř stejná pravidla od poloviny 90 let:
- vůči stanicím nelze otevírat spojení,
- vůči serverům jen povolené služby,
- SMTP ven jen z poštovních serverů,
- blokování MS Network, P2P sítí,
- stavový firewall,
- blokování phishingových/malware webů

45

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Segmentace sítě

- Firewall/router odděluje jednotlivé části sítě (VLAN),
- Cíle (bezpečnostní):
  - omezit útoky na linkové úrovni OSI modelu,
  - úspěšný útok na jeden prvek nemusí znamenat kompromitaci celé sítě,
  - zjednodušit pravidla (např. při umístění IP telefonů do jednoho segmentu)
- Techniky/postupy:
  - rozdělení zařízení uživatelů dle oprávnění – zvlášť zaměstnanci, zvlášť učebny, zvlášť eduroam, zvlášť koleje
  - servery dle služeb – zvlášť studijní systém, zvlášť knihovní systém, …
  - speciální zařízení do samostatných segmentů – IP telefony, IP kamery, telefonní ústředny, switche, hw sondy, ...
  - přiřazení pravidel dle uživatelských oprávnění – ve WiFI, na VPN, proxy servery a firewally s autentizací

46

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Proxy

Kdy použít **forward proxy**:

- filtrování přístupu,
- filtrování obsahu (filtrování reklam, blokování sociálních sítí, …),
- urychlení odpovědí (*v některých případech*),
- prokázání souladu s pravidly,
- skrytí interní sítě (*částečně*),
- anonymizace (*vhodnější je VPN*),

Kdy použít **reverse proxy**:

- load balancing (TCP multiplexing),
- podpora TLS, SSL Offload, SSL Acceleration,
- caching, zrychlení odpovědí,
- sloučení obsahu z více aplikací,
- aplikační firewall,
- autentizace, podpora single sign on

47

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Systém detekce průniku

- Intrusion detection system (IDS)
- Detekce neobvyklých aktivit, které by mohly vést k narušení bezpečnosti či být příznakem narušení bezpečnosti,
  - např. skenování portů může předcházet útoku,
- **Analyzovaná aktivita**:
  - na síti – Network intrusion detection systems (NIDS)
  - v operačním systému – Host intrusion detection systems (HIDS)
- **Detekce**:
  - pomocí pravidel,
  - pomocí signatur
  - detekce anomálií
- Systém musí při detekci generovat varování (**alert**):
  - zapsat do logu,
  - upozornit správce,
  - zablokovat aktivitu

48

Poznámky:

.....

.....

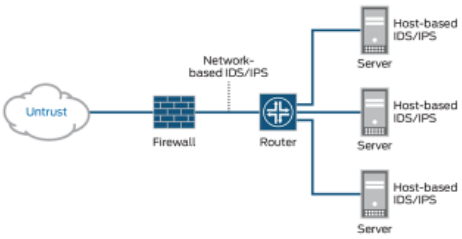
.....

.....

fis.vse.cz fisvse

Systém prevence průniku

- Intrusion prevention system (IPS)
- Detekce škodlivé činnosti, následné zablokování a nahlášení,
- tj. v principu IDS s tím, že je doplněn o bezpečné **provádění akcí** (zablokování provozu, vypnutí aplikace, vypnutí serveru)
- Často kombinace IDS/IPS



49

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

VPN

Virtuální privátní síť (VPN, Virtual Private Network)

- privátní propojení přes otevřenou síť,
- obvykle je součástí autentizace a šifrování provozu přes otevřenou síť,

Typy VPN:

- **Site-to-Site** – propojení podsítí skrz veřejnou síť,
  - připojení poboček,
  - připojení obchodních partnerů,
- **Remote Access** (host to network)
  - připojení stanice (zařízení) do podnikové sítě,
  - připojení k domácí síti,
- **Public VPN** – veřejní poskytovatelé VPN služeb,
  - změna lokality (obcházení omezení hlavně audiovizuálních služeb),
  - ochrana soukromí,
  - zvýšení bezpečnosti (nezabezpečené WiFi sítě),
  - obcházení firewallů (státních firewallů),

50

Poznámky:

.....

.....

.....

.....

fis.vse.cz fisvse

Anonymita

- **Anonymita**
  - situace, kdy není známá identita osoby, osoba je nedostupná či nedohledatelná
  - ochrana soukromí, svobody vs porušování zákonů
- **Anonymita na internetu**
  - internet není navržen s cílem zajistit anonymitu – ip adresa je identifikátor,
  - anonymní sítě – **tor** (the onion routing), i2p (invisible internet project), freenet, …
  - anonymní služby – anonymní remailer (odeslání/přesměrování pošty),
  - ochrana oznamovatelů protiprávních jednání (whistleblowers)
  - https://ssd.eff.org/ - surveillance self-defense

51

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Zero trust security

Módní pojem, takže mnoho různých občas protichůdných vysvětlení.

- začátky okolo roku 2004
- pojem poprvé v roce 2010
- medializace od 2016

Problém:

- nelze nadefinovat vnitřní (důvěryhodnou) síť a útočníky nechat „venku"

Myšlenky (**mindset**):

- neexistuje bezpečná (důvěryhodná) síť, požadavek ze známé sítě nemusí být bezpečný
- vše (téměř vše) je dostupné z Internetu, služby se přesouvají do cloudu
- více zdrojů důvěry (autentizace, místo, registrované zařízení, ...)
- předpokládat, že narušení je možné či že k němu došlo
- základem bezpečnosti je využívání standardů
- je nedostatek lidí na zajištění bezpečnosti

52

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Log, logování

Log – záznam o nějaké činnosti programu

Cíle:

- záznamy o využití aplikace,
- auditování operací a uživatelů,
- vývoj (ladění) aplikace, analýza chyb,
- obnova po pádu/chybě – transakční logy,

Logování:

- na chybový výstup (STDERR),
- do souboru,
- přes log protokol (přes log API),
- sondy – dotazují se pravidelně na stav procesu/OS,
- HW sondy (sensory, data loggers) – monitorování prostředí: teplota, vlhkost, počasí, provoz

53

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Zálohování dat (backup)

Záloha – kopie dat uložená na jiném datovém nosiči, na jiném místě

Archivace – dlouhodobé uchování dat,

Synchronizace dat – zajistit, aby na nějaké množině úložišť byla udržována stejná a aktuální data

zálohování	archivace
cílem je rychlá obnova měnících se dat	ukládají se data, která se již nemění (při ukončení projektu)
existují kopie na více zařízeních	obvykle jedna kopie
rychlost obnovy je podstatná	důležitá je možnost náhledu na údaje a prokázání integrity
krátkodobé uložení záloh	dlouhodobé uložení
duplicitní kopie jsou přepisovány	nedochází k přepisu dat

54

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

Základy odborné práce

Repetitorium pro přijímací zkoušky

Věra Radváková

Vysoká škola ekonomická v Praze

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Analytické myšlení

- **Analytické** myšlení znamená, že můžeme systém **rozložit** a zabývat se jeho částmi samostatně. Při analytickém myšlení to, co chceme pochopit, rozkládáme na části.
- Při syntetickém myšlení naopak to, co chceme pochopit, chápeme jako součást většího celku. Při analýze rozložíme firmu na různá oddělení, při syntéze ji chápeme jako součást průmyslového odvětví nebo celé společnosti.
- V dnešní době se nejčastěji používá termín **kritické myšlení**, což znamená ***nepodléhat obecnému mínění, naivně nepřebírat názory, připustit odlišný pohled, a především vytvořit si názor na základě vědomostí a zkušeností.*** Samozřejmou součástí kritického myšlení je analytické myšlení.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Informační etika

- V informační etice stojíme před mnoha problémy. Patří sem např. obtíže s definicí informace, jež je nutná k odhalení jejích etických souvislostí, dále není jasné, jakou kontrolu by měl tvůrce informace nad ní mít, k jakým informacím by měli mít ostatní přístup, do jaké míry mají subjekty právo na srozumitelnou, dostupnou a přesnou informaci atd.
- V dnešní době plné informací není možné **získat informaci** a tuto informaci okamžitě použít. Prvně je nutné dané informaci řádně **porozumět**, poté informaci **ověřit,** dát do souvislostí a až v tuto chvíli může autor novou informaci **použít** v rámci své odborné práce.

Poznámky:

.....

.....

.....

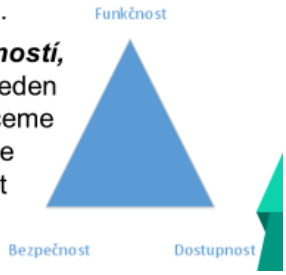
.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Etické problémy v kyberprostoru

- Informační etika se zabývá etickými problémy ve vědecké práci, v médiích, informační vědě, ICT, řízení informačních systémů, internetu atd. V současnosti je nutné vidět etické problémy v souvislosti v celém kyberprostoru.
- V kyberprostoru existuje vztah mezi ***bezpečností, dostupností a funkčností***. Pokud se zvýší jeden aspekt, úroveň ostatních se sníží. Pokud chceme vytvořit maximálně bezpečný systém, musíme například omezit jeho funkčnost a dostupnost pro uživatele.



Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Kybernalita

- Kybernalitou rozumíme kriminální činnost, která může být namířena přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod., nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu. Společnost bývá ke kybernalitě tolerantnější než ke klasické kriminalitě.
- **Problém 1** = etický i právní. Právo ani etické normy se nestačí dostatečně rychle přizpůsobovat měnícímu se technologickému prostředí.
- **Problém 2** = samotné odhalení kybernality. Vyžaduje speciální vybavení, znalosti a postupy.
- **Problém 3** = společenský. Neetické a nelegální chování týkající se informací má často nehmotnou povahu, takže je skrytější. Často těžko zjistitelné a odhalitelné, navíc společností více tolerované.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Citační etika

Způsob citování a vytvoření bibliografických odkazů určují mezinárodní normy:

- **citační norma APA**, které odpovídají ISO 690: *Documentation – Bibliographie reference – Content, form and structure* ISO 690-2: *Information and documentation-Bibliographic reces-Part 2: Electronic documents,*
- prvky citace se dělí na **povinné** a **nepovinné** (základní bibliografická citace, rozšířená bibliografická citace). Povinnými prvky citace jsou: **autor, název díla, rok vydání, místo a nakladatelství.**

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Citační etika

- Uvést všechny použité prameny a zdroje.
- Uvést přesnou a úplnou citaci.
- Dát odkazy z textu na seznam použitých zdrojů.
- Přehlednost a jednotnost.
- Přesnost a úplnost.
- Zachovat jazyk knihy.
- Chybějící údaje vynechat, nedomýšlet.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Typy citace

- **Doslovná citace**

Autor v práci uvede doslovně text práce jiného autora Doslovná citace je psána kurzívou.

Příklad 1: … tyto výsledky komentuje Petr Novotný slovy: *Výběr vzorků pro testování se ukázal jako rozhodující, dosažené výsledky proto nemusí být reprezentativní* (Novotný, 2008, s. 46). S ohledem na současnou situaci ...

- **Parafrázovaná citace**

Autor v práci uvádí pouze myšlenky a závěry, které byly publikovány v cizí práci. Parafrázovaná citace není kurzívou.

Příklad 2: … Problematika e-learningu byla zkoumána nejprve v prostředí univerzit (Stefan, 2007), později i v prostředí komerčních firem v USA (Novotný, 2008) …

Popřípadě odkazy mohou být až na konci podkapitoly.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

IMRaD - struktura odborné práce

MOTIVACE		VÝSLEDKY
	METODA	
CÍLE		ZÁVĚRY

IMRaD zkratka Introduction, Methods, Results a Discussion je povinné členění odborného textu. V odborné komunitě je to de facto norma.

Úvod / Introduction
- téma, cíl, motivace
- současný stav poznání
- výzkumné otázky

Metody / Methods
- použité nástroje (kvantitativní/kvalitativní)
- způsob získání dat, rozsah vzorku, …
- zpracování dat

Výsledky / Results
- získaná data a výsledky výpočtů
- interpretace výsledků
- odpovědi na výzkumné otázky

Diskuze / Discussion
- diskuze nad výsledky
- vyvození závěrů
- potvrzení/vyvrácení hypotéz

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Základní struktura odborné práce

- **Úvod** je uvedení do tématu, problematiky, kterou bude autor v práci řešit. Nelze zaměňovat s předmluvou. Úvod by měl rozvést zvolené téma, stručně ho zasadit do souvislostí a odpovědět na otázku, proč bylo toto téma zvoleno, tedy zdůvodnit jeho nutnost, aktuálnost. Často důležitou částí úvodu je stanovení cíle práce a metody zpracování. Někteří autoři do úvodu uvádějí především motivaci k sepsání práce a pro cíl a metody vytvářejí samostatnou podkapitolu. V odborných knihách se úvod a závěr **nečísluje.**
- **Text** odborné práce se člení do **kapitol, podkapitol**, odstavců. Začátek nové kapitoly by měl být na nové stránce. Části práce se označují arabskými číslicemi, přičemž se začíná od jedničky. Mezi čísla, označující různé stupně členění textu se klade tečka.
- **Závěr** je nejdůležitější část práce, obsahuje shrnutí práce, odpovídá na míru splnění cíle, který byl stanoven, případně shrnuje odpovědi na otázky, které byly položeny v úvodu práce. V závěru by měla být i další doporučení.
- **Seznam zdrojů** (popř. seznam literatury) se nachází na konci každé odborné práce, nezáleží na rozsahu. Jde o souhrn údajů o citované publikaci, umožňující její identifikaci.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Základní pojmy

- **Abstrakt** je autorský souhrn odborného textu, tedy shrnutí celé stati nebo knihy. Obsahuje cíle, metody zpracování, výsledky a nové poznatky, ke kterým autor dospěl. Rozsah abstraktu bývá 150 – 250 slov. Při stylizaci se používají celé věty, slovesa v činném rodě a ve třetí osobě. Musí být velmi hutný a důsledný, neboť v dnešní době informační exploze se čtenář často spokojí právě s přečtením abstraktu a teprve na jeho základě se rozhoduje, zda stojí za to číst celý text. V abstraktu se neužívají citace ani parafráze z daného textu. Bývá v českém a anglickém jazyce. Ve vědecké práci se řadí před obsah. Abstrakt je povinná součást každé vědecké práce.
- **Klíčová slova** jsou nejdůležitější termíny, kterými autor co nejvýstižněji charakterizuje obsah odborné práce. Počet klíčových slov je různý, většinou se vejdou na jeden až dva řádky. Uvádějí se mimo jiné i pro zařazení odborné práce do indexových a abstraktových služeb.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Základní pojmy

- **Anotace** se někdy zaměňuje za pojem abstrakt a představuje vlastně faktografickou informační podstatu primárního dokumentu. Anotace není úplný odborný text, bývá součástí abstraktu spolu s bibliografickou citací.
- **Teze** je zhuštěný výklad hlavních myšlenek teprve připravované publikace, vědecké práce. Při stylizaci se nemusí používat celé věty, stačí dílčí cíle, metody, případné rešerše předložit v jednotlivých bodech.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Základní pojmy

- **Rešerše** je sekundární dokument. Jedná se o soupis subjektivně nejdůležitějších bodů a myšlenek odborného textu, který napsal jiný autor. Pod označením rešerše chápeme prakticky jakoukoli cestu vedoucí k získání informací na dané téma. Rešerše slouží k rychlému pochopení a orientaci v tématu, vytváří osnovu textu.
- **Vědecká stať** je odborný žánr, ve kterém autor koncipuje vlastní, nové řešení problému či tématu. Vědecké statě jsou i **závěrečné studentské kvalifikační práce.**

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Metoda – metodika - metodologie

- **Metodika** je promyšlený postup při práci (odráží přístup autora k řešení zadaného tématu).
- **Metody** jsou konkrétní způsoby a aplikace postupu (metoda je nástroj ke zkoumání daného výzkumného předmětu).
- **Metodologie** je věda o metodách. Metodologie je teorií k výběru výzkumných metod, je také návodem, jak vybrané metody používat k vědeckému zkoumání.

Poznámky:

.....

.....

.....

.....

VŠE / FAKULTA INFORMATIKY A STATISTIKY

fis.vse.cz fisvse

Empirický výzkum

- **Základní výzkum** - cílem je získat znalosti o základech či podstatě pozorovaných jevů, vysvětlení jejich příčin a možných dopadů při využití získaných poznatků.
- **Aplikovaný výzkum** - cílem je získání nových poznatků zaměřených na budoucí využití v praxi.

Základní typy empirického výzkumu

- **kvantitativní** = statistické šetření
- **kvalitativní** = zkoumá zkušenosti a názory respondentů, statisticky velmi špatně uchopitelné

Poznámky:

.....

.....

.....

.....

Poznámky:

.....

.....

.....

.....

Učebnice k přípravám na přijímací zkoušky

DOUCEK, Petr, MARYŠKA, Miloš, NEDOMOVÁ, Lea. *Informační management v informační společnosti.* 1. vyd. Praha : PROFESSIONAL PUBLISHING, 2013. 264 s. ISBN 978-80-7431-097-3. (Další autoři: DIANIŠ, Erik, MATUŠTÍK, Ondřej, OŠKRDAL, Václav, PAVLÍČEK, Antonín, SKRBEK, Jan, STŘÍŽOVÁ, Vlasta)

PAVLÍČEK, Antonín, GALBA, Alexander, HORA, Michal. *Moderní informatika.* 2. rozšíř. vyd. Praha : Professional Publishing, 2017. 199 s. ISBN 978-80-906594-6-9.

RADVÁKOVÁ, Věra, LÖSTER, Tomáš, MAZOUCH, Petr, SIGMUND, Tomáš, VLTAVSKÁ, Kristýna. *Metody vědecké práce [online]*. 1. vyd. Praha : Oeconomica, 2018. 134 s. ISBN 978-80-245-2249-4. Dostupné z: http://www.ekopress.cz/titdetail.php?tid=30927

RADVÁKOVÁ, Věra, SIGMUND, Tomáš. *Základy odborné práce.* 2. aktual. a rozšíř. vyd. Praha : Oeconomica, Nakladatelství VŠE, 2020. 164 s. ISBN 978-80-245-2404-7

Stránky našeho nakladatelství
http://oeconomica.vse.cz/

Název	**REPETITORIUM PRO INFORMAČNÍ MANAGEMENT** **Materiály pro přípravu k přijímacímu řízení na navazující magisterský studijní program Informační management**
Autoři	PhDr. Ing. Antonín Pavlíček, Ph.D. Ing. Richard Novák, Ph.D. Ing. Luboš Pavlíček PhDr. Věra Radváková, Ph.D. Mgr. Jana Syrovátková
Vydavatel	Vysoká škola ekonomická v Praze Nakladatelství Oeconomica
Doporučeno	pro magisterské studium na VŠE v Praze
Vydání	1. vydání v elektronické podobě
Návrh obálky	Daniel Hamerník, DiS.
Počet stran	98
DTP	Vysoká škola ekonomická v Praze Nakladatelství Oeconomica
Sazba	autoři

Tato publikace neprošla redakční úpravou.
Zdarma ke stažení

ISBN 978-80-245-2447-4