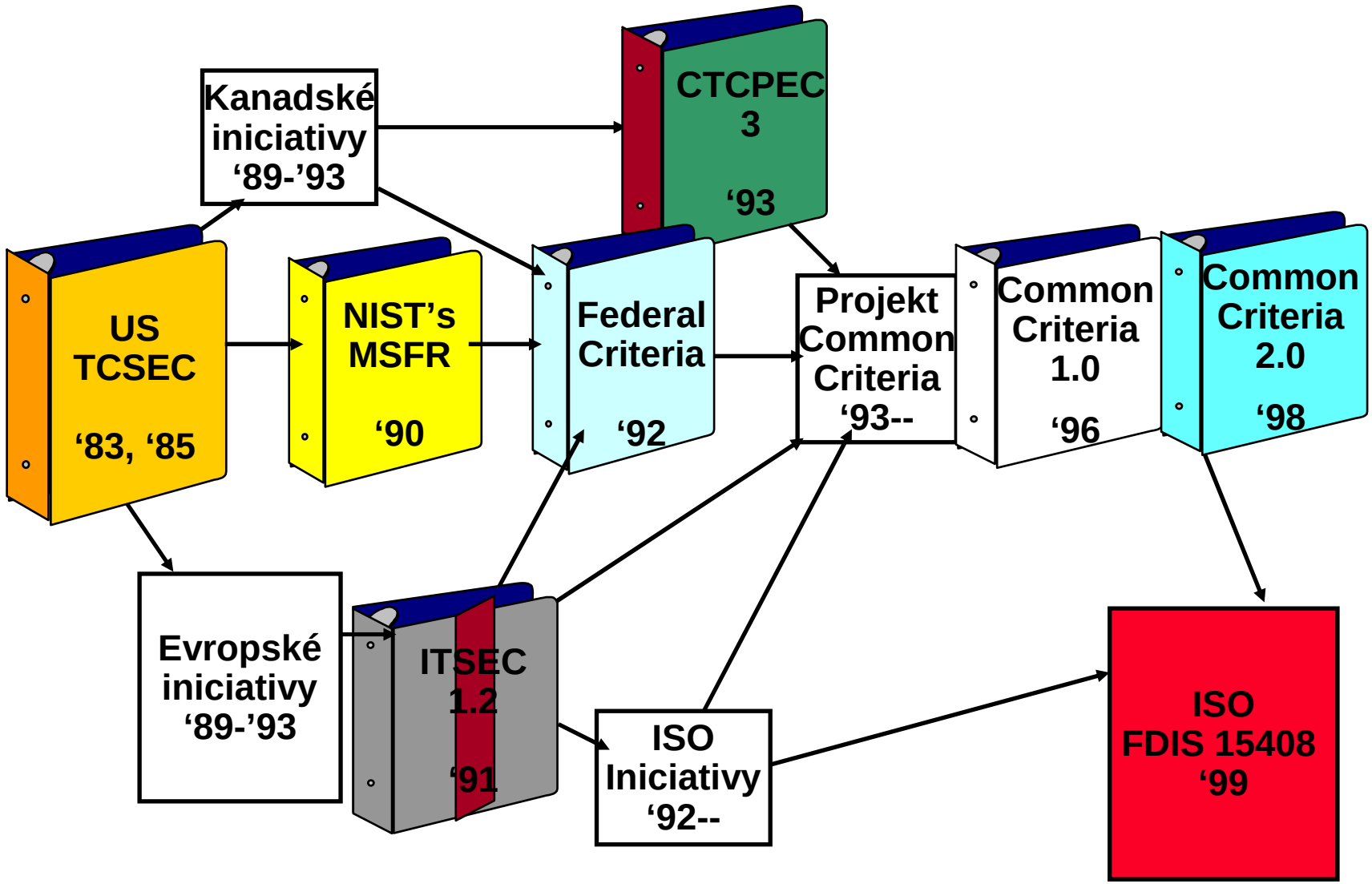
Act 2007

BIS
Bezpečnost informačních systémů

Petr Hanáček
Faculty of Information Technology
Technical University of Brno
Božetěchova 2
612 66 Brno
tel. 5 4114 1216
e-mail: hanacek@fit.vutbr.cz

Kritéria hodnocení bezpečnosti IS

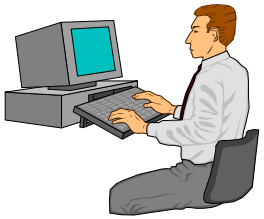
Historie kritérií bezpečnosti IT



Pro koho jsou kritéria určena

- Uživatelé

- Vývojáři



- Hodnotitelé

- Jiní ...

Kritéria se nezabývají:

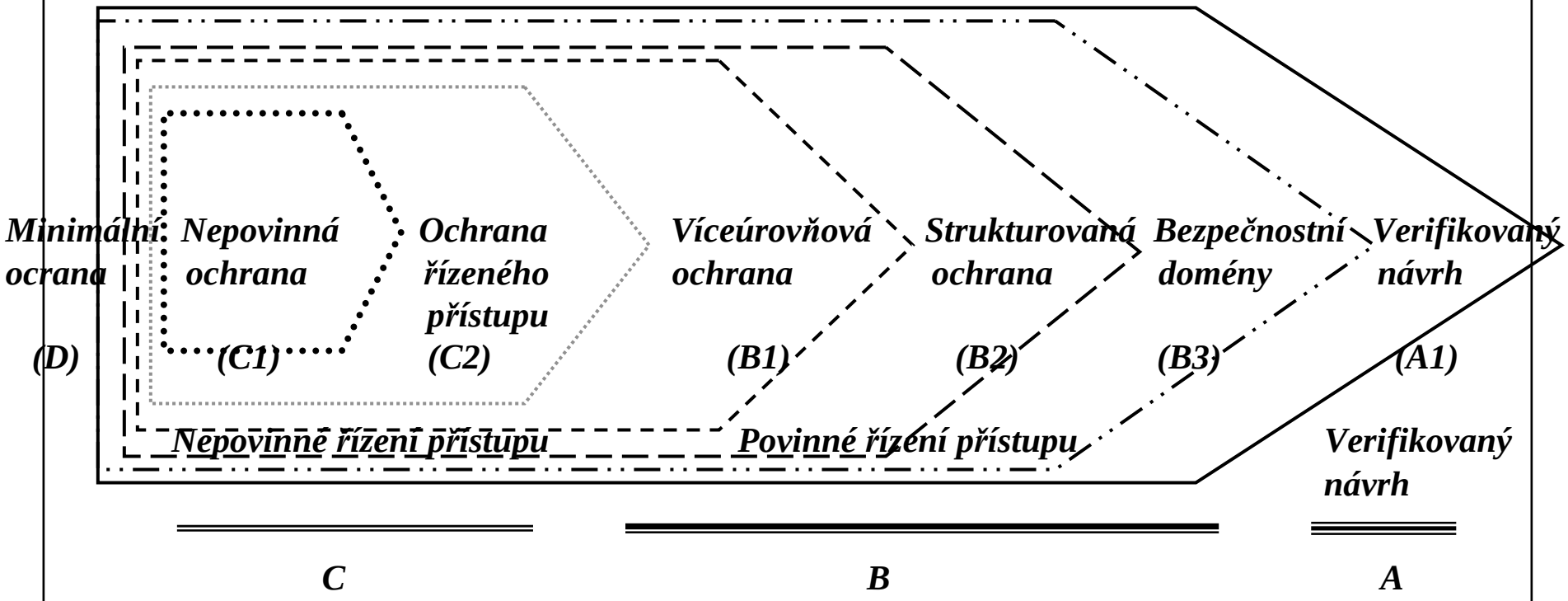
- **...administrativními opatřeními**
- **...fyzickými aspekty bezpečnosti IT**
- **...metodologií hodnocení**
- **...dohodami o vzájemném uznávání**
- **...kryptografickými *algoritmy***
- **...akreditací**

Orange Book

Rainbow series

- **Orange**
  - **Trusted Computer System Evaluation Criteria (TCSEC)**
- **Yellow**
  - **Guidance for Applying the Orange Book**
- **Red**
  - **Trusted Network Interpretation (TNE)**
- **Lavender (levandule)**
  - **Trusted Database Interpretation**

Úrovně TCSEC



Požadavky úrovní

- **C1: Discretionary Protection**
  - Identifikace
  - Autentizace
  - Nepovinné řízení přístupu
- **C2: Controlled Access Protection**
  - Opětné použití a audit
- **B1: Labeled security protection**
  - Povinné řízení přístupu pro některé objekty
  - Neformální model bezpečnostní politiky
- **B2: Structured Protections**
  - Důvěryhodná cesta pro přihlášení
  - Princip nejmenších privilegií
  - Formální model bezpečnostní politiky
  - Analýza skrytých kanálů
  - Správa konfigurace
- **B3: Security Domains**
  - Mechanismus validace referencí (referenční monitor)
  - Omezení při vytváření kódu
  - Požadavky na dokumentaci a testování
- **A1: Verified Protection**
  - Formální metody pro analýzu a verifikaci
  - Důvěryhodná distribuce

Oblasti TCSEC

- **Bezpečnostní politika**
- **Účtovatelnost**
- **Zaručitelnost**
- **Dokumentace**
- **Analýza skrytých kanálů**
- **Architektura systému**
- **Specifikace a verifikace návrhu**

Bezpečnostní politika

	C1	C2	B1	B2	B3	A1
Nepovinné řízení přístupu (DAC)	+	+	nc	nc	+	nc
Opětné použití	0	+	nc	nc	nc	nc
Klasifikace dat (Labels)	0	0	+	+	nc	nc
Integrita klasifikace	0	0	+	nc	nc	nc
Export klasifikace	0	0	+	nc	nc	nc
Klasifikace neelektronických výstupů	0	0	+	nc	nc	nc
Povinné řízení přístupu (MAC)	0	0	+	+	nc	nc
Úroveň prověření uživatelů	0	0	0	+	nc	nc
Klasifikace zařízení	0	0	0	+	nc	nc

0	Žádné požadavky
+	Dodatečné požadavky
nc	Beze změny

Účtovatelnost

	C1	C2	B1	B2	B3	A1
Identifikace a autentizace	+	+	+	nc	nc	nc
Audit	0	+	+	+	+	nc
Důvěryhodná cesta	0	0	0	+	+	nc

0	**Žádné požadavky**
+	**Dodatečné požadavky**
nc	**Beze změny**

Zaručitelnost

	C1	C2	B1	B2	B3	A1
Architektura systému	+	+	+	+	+	nc
Integrita systému	+	nc	nc	nc	nc	nc
Testování	+	+	+	+	+	+
Specifikace a verifikace návrhu	0	0	+	+	+	+
Analýza skrytých kanálů	0	0	0	+	+	+
Správa důvěryhodných zařízení	0	0	0	+	+	nc
Správa konfigurace	0	0	0	+	nc	+
Důvěryhodné zotavení	0	0	0	0	+	nc
Důvěryhodná distribuce	0	0	0	0	0	+

0	Žádné požadavky
+	Dodatečné požadavky
nc	Beze změny

Dokumentace

	C1	C2	B1	B2	B3	A1
Uživatelská dokumentace	+	nc	nc	nc	nc	nc
„Manuál důvěryhodných zařízení“	+	+	+	+	+	nc
Dokumentace k testům	+	nc	nc	+	nc	+
Dokumentace k návrhu	+	nc	+	+	+	+

0	Žádné požadavky
+	Dodatečné požadavky
nc	Beze změny

Analýza skrytých kanálů

B1	**Bez požadavků**
B2	**Paměťové skryté kanály**
B3	**Všechny (paměťové i časové) skryté kanály**
A1	**Formální metody**

Architektura systému

C1	**DVB musí být schopna ochránit sama sebe**
C2	**DVB musí izolovat jednotlivé prostředky, o které se stará**
B1	**DVB musí zajistit dokonalou izolaci procesů**
B2	**DVB musí být strukturovaná do nezávislých, dobře definovaných modulů**
B3	**Návrh DVB musí využívat principy vrstevnatosti, abstrakce a skrývání dat**
A1	**Žádné dodatečné požadavky**

Specifikace a verifikace návrhu

C2 Žádné požadavky

B1 Neformální nebo formální model bezpečnostní politiky

B2 Formální model bezpečnostní politiky u kterého je dokázaná konzistence

DTLS (descriptive top-level specification) modulu DVB

B3 DTLS musí být prokazatelně konzistentní s modelem

A1 FTLS (formal top-level specification) modulu DVB

FTLS musí být prokazatelně konzistentní s modelem

DTLS musí být prokazatelně konzistentní s modelem

Neoficiální pohled na úrovně

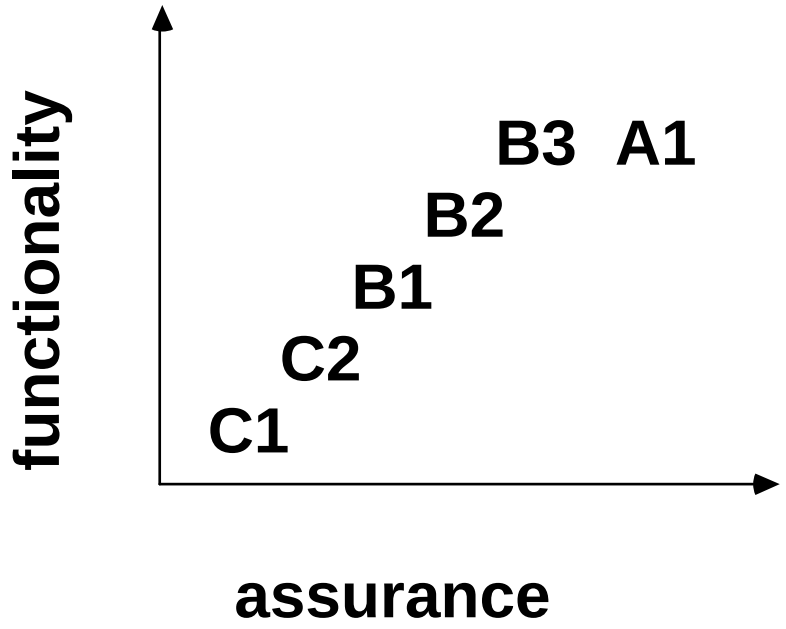
- **C1, C2**
  - **Prosté vylepšení existujících systémů. Neohrožuje aplikace.**
- **B1**
  - **Závažnější rozšíření existujících systémů (především MAC). Některé aplikace vyžadují úpravy.**
- **B2**
  - **Zásadní změny oproti stávajícím systémům. Většina aplikací beze změn nebude fungovat.**
- **B3**
  - **Typicky systémy, které nezvládly A1**
- **A1**
  - **Systém musí být navržen a implementován od základu. Nutné využití entradičníc metod.**

Nedostatky TCSEC

- **Směšuje v jednom dokumentu různé úrovně abstrakce**
- **Málo se zabývá integritou dat**
  - **Vojenský původ**
- **Kombinuje funkčnost a zaručitelnost do jedné lineární stupnice**
- **Nezná komunikaci a počítačovou síť**
  - **Publikace Trusted Network Interpretation (TNE) je nepoužitelná**

Funkčnost a zaručitelnost

- **TCSC nerozlišuje funkčnost a zaručitelnost**
- **Funkčnost (functionality)**
  - **Co je implementováno**
- **Zaručitelnost (assurance)**
  - **Jaká je míra důvěry, že je to správně**
  - **Lineární stupnice**



Příklady ohodnocených produktù

- **A1 - Secure Communications Processor (SCOMP), Release 2.1, Honeywell**
- **B2 - Multics MR11.0, Honeywell**
- **B1 - UNIX System V/MLS, Release 1.1.2 AT&T**
- **C2 - VAX/VMS Version 4.3 DEC**
- **C2 - SunOS, instalovaný pro C2 Sun Microsystems**

UNIX ve třídě C2

Oproti standardnímu UNIXU je třeba změnit:

- **opětné použití objektù**
  - » **disk, paměť, obrazovka**
- **NCSC prohlásilo, že řízení přístupu vyhovuje C2**
- **audit**
  - » **všechna přihlášení a odhlášení uživatelů**
  - » **všechny akce prováděné správcem**
  - » **maximální ochrana auditních dat**
  - » **oddělení auditních záznamù**
- **zašifrovaná hesla nesmí být přístupná (shadow)**
- **použitý procesor musí zajistit oddělení procesů**
- **3 bezpečnostní příručky (uživatel, administrátor, technický popis)**

NCSC - National Computer Security Center

Index rizika

- **prostředek pro vyjádření požadované úrovně bezpečnosti**
  - **R_{min} - minimální úroveň prověření uživatele**
  - **R_{max} - maximální úroveň citlivosti dat**
  - **Index rizika = R_{max} - R_{min}**

prověření uživatele	R_{min}
Neprověřený	0
Příst. k citlivým inf.	1
Prověřen pro důvěrné	2
Prověřen pro tajné	3
Prověřen pro přísně tajné	4

citlivost dat	R_{max}
Neklasifikovaná	0
Neklasifikovaná, citlivá	1
Důvěrná	2
Tajná	3
Přísně tajná	4

Index rizika (pokr.)

- **minimální třída bezpečnosti systému pro daný index rizika:**

Index rizika	otevřené prostředí	uzavřené prostředí
0	C2	C2
1	B1	B1
2	B2	B2
3	B3	B2
4	A1	B3
5	-	A1

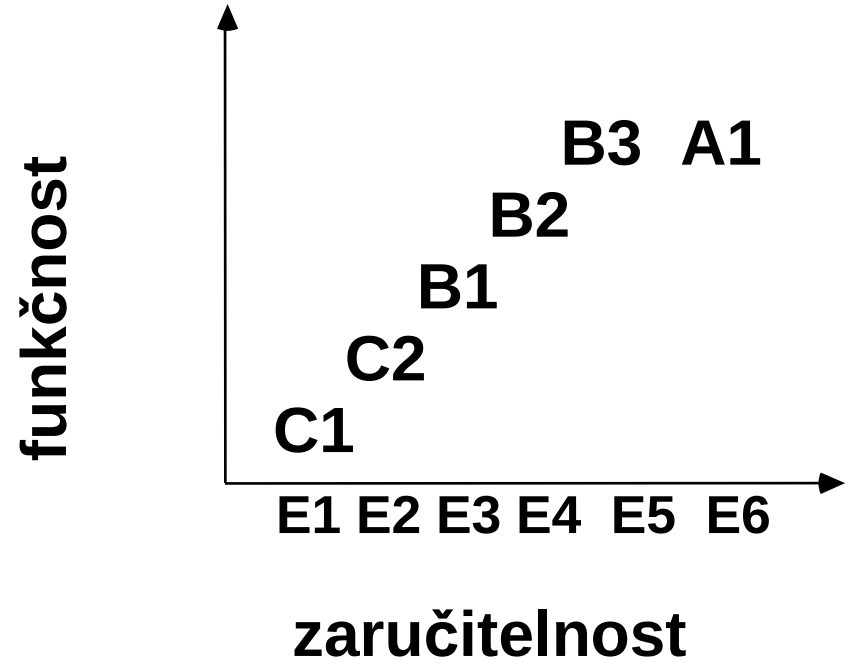
ITSEC

ITSEC

- **ITSEC: IT Security Evaluation Criteria**
- **Vytvořena z národních kritérií UK, Německa, Francie a Holandska**
- **Výstupy**
  - **ITSEC: 1991**
  - **ITSEM: 1993 (IT Security Evaluation Manual)**
  - **UK IT Security Evaluation & Certification scheme: 1994**

ITSEC - Metodologie

- **Založené na systematickém a dokumentovaném přístupu k hodnocení**
- **Rozlišují produkty a systémy**
- **Dva rozměry**
  - **Funkčnost**
  - **Zaručitelnost**



ITSEC – Třídy funkčnosti

- **Přístup 1:**
  - **F-C1, F-C2, F-B1, F-B2, F-B3**
  - **Třídy odpovídající stejnojmenným úrovním TCSES**
- **Přístup 2:**
  - **F-IN**
    - » **Systémy se zvýšenými nároky na integritu**
  - **F-AV**
    - » **Systémy se zvýšenými nároky na dostupnost**
  - **F-DI**
    - » **Systémy se zvýšenými nároky na integritu přenosu dat**
  - **F-DC**
    - » **Systémy se zvýšenými nároky na důvěrnost přenosu dat**
  - **…**

ITSEC - Zaručitelnost

- **E1: Security target defined, tested**
  - **Must have informal architecture description**
- **E2: Informal description of design**
  - **Configuration control, distribution control**
- **E3: Correspondence between code and security target**
- **E4: Formal model of security policy**
  - **Structured approach to design**
  - **Design level vulnerability analysis**
- **E5: Correspondence between design and code**
  - **Source code vulnerability analysis**
- **E6: Formal methods for architecture**
  - **Formal mapping of design to security policy**
  - **Mapping of executable to source code**

ITSEC - síla mechanismů

- **Síla mechanismů je podle ITSEC (odstavce 3.6-3.8):**
  - **základní**
  - **střední**
  - **vysoká**
- **Význam:**
  - **a) <u>základní</u>**
    mechanismus chrání proti náhodným poruchám, avšak může být narušen kvalifikovanými útočníky.
  - **b) <u>střední</u>**
    mechanismus chrání proti útočníkům s omezenými příležitostmi a prostředky.
  - **c) <u>vysoká</u>**
    mechanismus může být narušen pouze útočníky, disponujícími vysokou úrovní znalostí, příležitostmi a prostředky rovněž na vysoké úrovni a úspěšný útok se vymyká běžné praxi.
- **Vágní definice - v praxi nepoužitelná**

ITSEM - síla mechanismů

- **Síla mechanismů bere v úvahu**
  - **znalosti**
  - **prostředky**
  - **příležitost útočníka**
- **Znalosti**
  - **vyjadřují míru vědění, kterou musí mít osoba, aby byla schopna zaútočit na HP.**
    - **Začátečník je ten, kdo nemá žádné zvláštní znalosti.**
    - **Zkušený je seznámený s interní činností HP.**
    - **Expert je seznámený s principy a algoritmy, použitými v HP.**
- **Prostředky**
  - **objem prostředků, které musí útočník vynaložit k úspěšnému útoku na systém. Jsou dvojí - čas a vybavení.**
    - » **Čas - doba, kterou útočník potřebuje na provedení útoku**
      - **v minutách - do deseti minut**
      - **ve dnech - do jednoho měsíce**
      - **v měsících - útok trvá více než měsíc**
    - » **Vybavení - počítače, elektronická zařízení, technické prostředky a programy.**
      - **bez vybavení - není potřebné žádné speciální vybavení**
      - **běžné vybavení - vybavení, které je běžně dostupné v provozním prostředí HP**
      - **speciální vybavení - speciální jednoúčelové vybavení**

- **Příležitost**
  - **zahrnuje faktory, které obecně není schopen útočník ovlivnit**
    - **požadavek na asistenci jiné osoby (komplot)**
    - **pravděpodobnost výskytu jisté speciální kombinace okolností (šance)**
    - **pravděpodobnost a následky odhalení útočníka (detekce)**
  - **formy komplotu:**
    - **samostatný, pokud žádný komplot není potřeba**
    - **s uživatelem, pokud je pro úspěch útoku třeba komplot mezi útočníkem a (nedůvěryhodným) uživatelem HP**
    - **se správcem, pokud je třeba komplot s vysoce důvěryhodným u ivatelem HP**
  - **Tato definice komplotu předpokládá, že útočník není autorizovaným uživatelem HP**

Tabulka pro čas a komplot

	samostatný	s uživatelem	se správcem
v minutách	0	12	24
ve dnech	5	12	24
v měsících	16	16	24

Tabulka pro znalosti a vybavení

	bez vybavení	běžné vybavení	speciální vybavení
začátečník	1	-	-
zkušený	4	4	-
expert	6	8	12

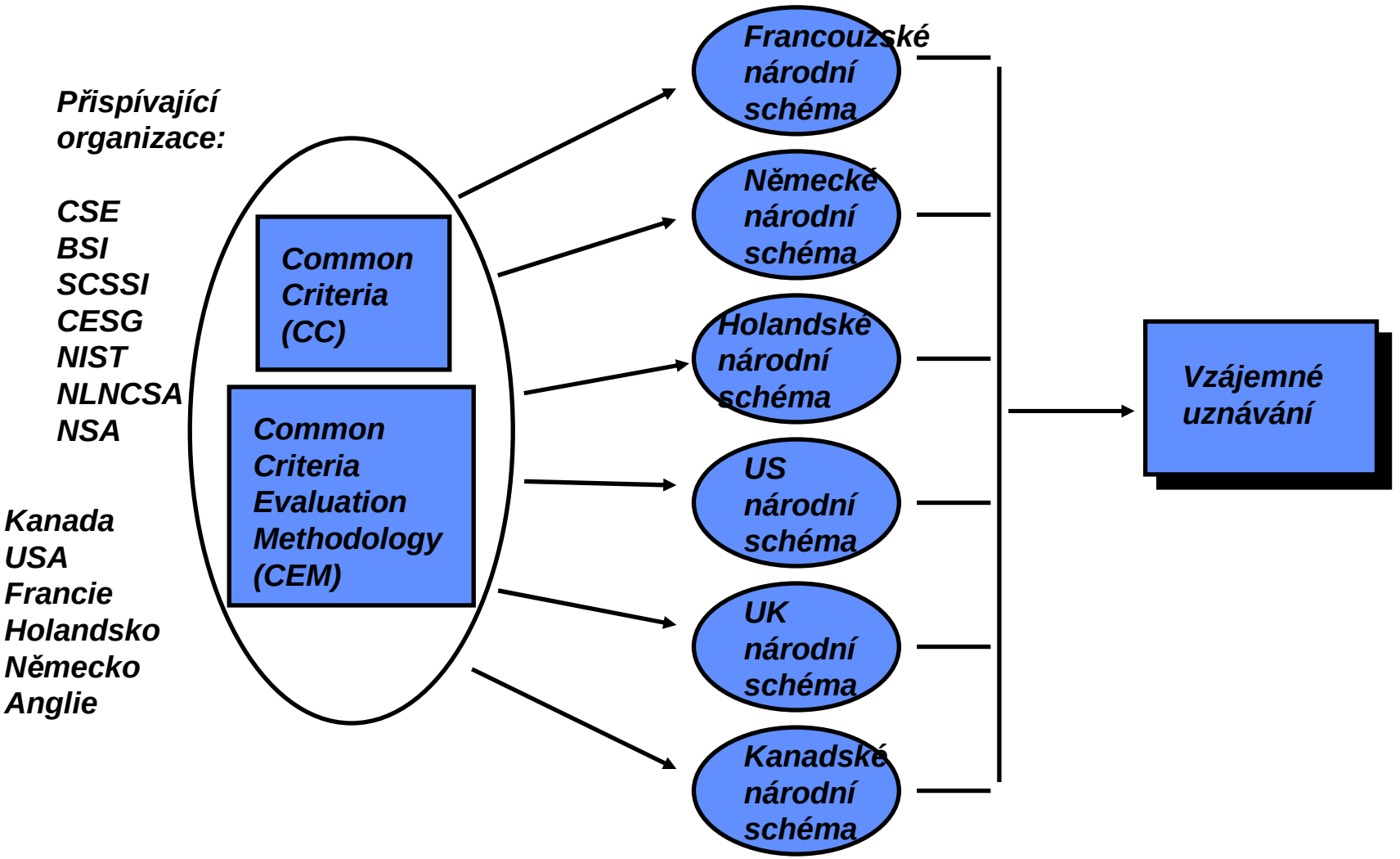
Je třeba sečíst hodnoty, získané z tabulek:

v=1	**síla není ani základní.**
1<v<12	**síla je základní.**
12<v<24	**síla je střední.**
24<v	**síla je vysoká.**

Hodnocení bezpečnosti IT podle normy ISO/IEC 15408 (Common Criteria)

Petr Hanáček
Fakulta informačních technologií
VUT Brno
hanacek@fit.vutbr.cz

Kontext kritérií



Struktura ISO 15408 / CC

Část 1
Úvod a použitý model

- Popis přístupu
- Pojmy a model
- Požadavky na profily ochrany bezpečnostní cíl

Část 2 Bezpečnostní funkční požadavky

- Třídy funkcí
- Rodiny funkcí
- Komponenty
- Detailní požadavky

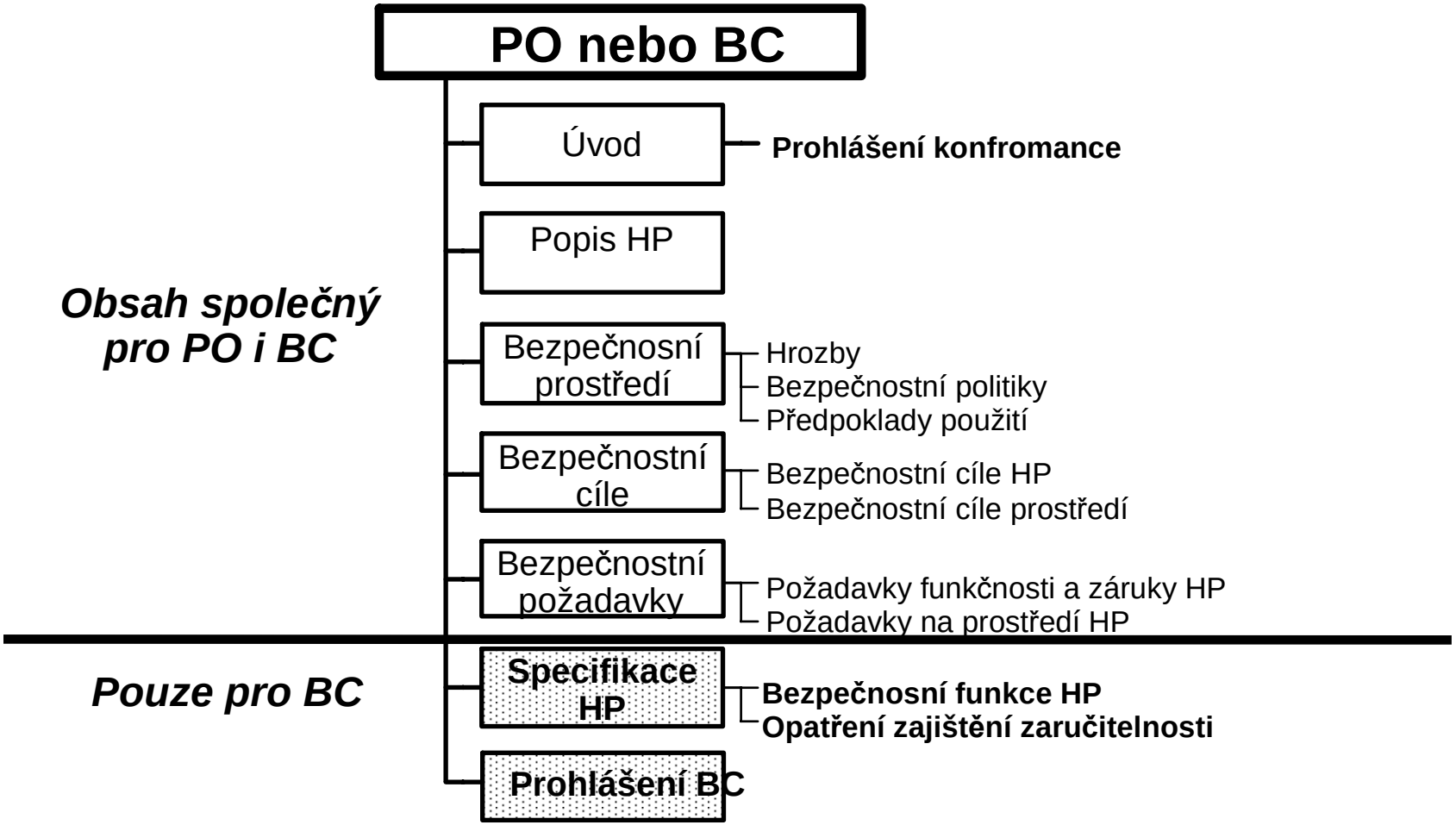
Část 3 Požadavky zaručitelnosti bezpečnosti

- Třídy zaručitelnosti
- Rodiny zaručitelnossti
- Komponenty zaručitelnosti
- Detailní požadavky
- Úrovnně zaručitelnosti EAL

Část 4
Registr profilů ochrany

Profil ochrany a bezpečnostní cíl

- **PO - Pro kategorii produktů**
- **BC - Pro konkrétní typ produktu**



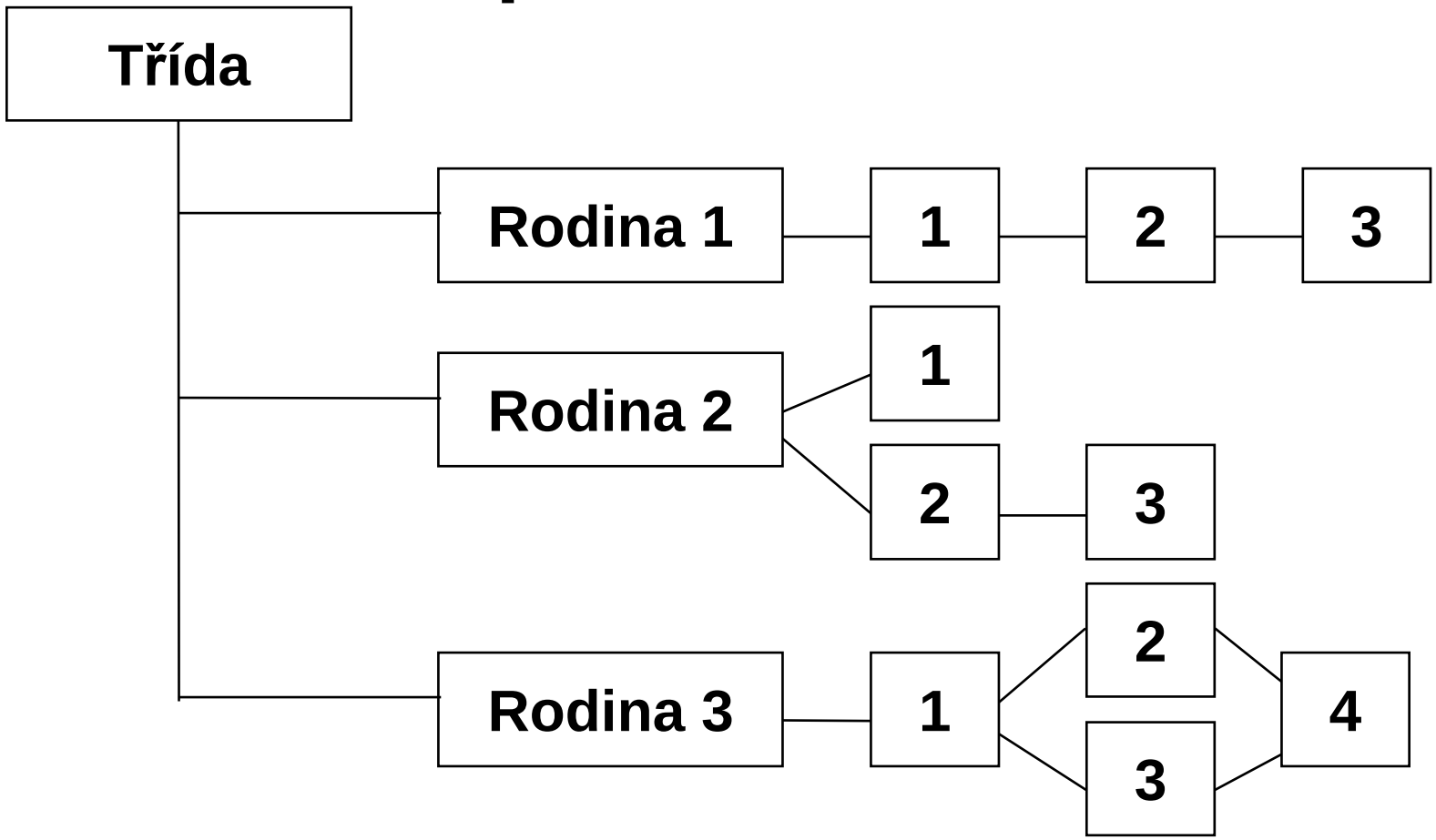
Část 2 - Třídy funkčních požadavků

- **Třída FAU: Bezpečnostní audit (35 komponent)**
- **Třída FCO: Komunikace (4)**
- **Třída FCS: Kryptografická podpora (40)**
- **Třída FDP: Ochrana uživatelských dat (46)**
- **Třída FIA: Identifikace a autentizace (27)**
- **Třída FMT: Správa bezpečnosti**
- **Třída FPR: Soukromí (8)**
- **Třída FPT: Ochrana bezpečnostní funkcionality (43)**
- **Třída FRU: Využití zdrojů (8)**
- **Třída FTA: Přihlášení do HP (11)**
- **Třída FTP: Důvěryhodné cesty/kanály (2)**

Hierarchie pojmů

- **Třída (např. FDP - Ochrana uživatelských dat): seskupení rodin, které jsou stejně zaměřeny**
- **Rodina (např. FDP_ACC - Politika řízení přístupu): seskupení komponent, které mají stejný bezpečnostní cíl ale různou sílu nebo přísnost**
- **Komponenta (např. FDP_ACC.1 - Řízení přístupu k podmnožinám):**
  nejmenší volitelná sada prvků, která může být použita v BC nebo PO

Část 2 - Hierarchie funkčních požadavků



Zaručitelnost - Assurance

- **Slovníková definice: (Oxford)**
  - **a positive declaration that a thing is true**
  - **a promise or guarantee**
  - **certainty**
- **Definice podle CC:**
  - ***grounds for confidence that an IT product or system meets its security objectives***
- **Je ochranou proti:**
  - **špatnému návrhu**
  - **implementačním chybám**
  - **neefektivním opatřením nebo mechanismům**

Část 3 - Evaluation Assurance Levels (EALs)

EAL	Jméno	*TCSEC
EAL1	funkčně testovaný	
EAL2	strukturálně testovaný	C1
EAL3	metodicky testovaný a kontrolovaný	C2
EAL4	metodicky navrhovaný, testovaný a přezkoumávaný	B1
EAL5	semiformálně navrhovaný a testovaný	B2
EAL6	testovaný se semiformálně ověřovaným návrhem	B3
EAL7	testovaný s formálně ověřovaným návrhem	A1

*TCSEC = “Trusted Computer Security Evaluation Criteria” --”Orange Book”

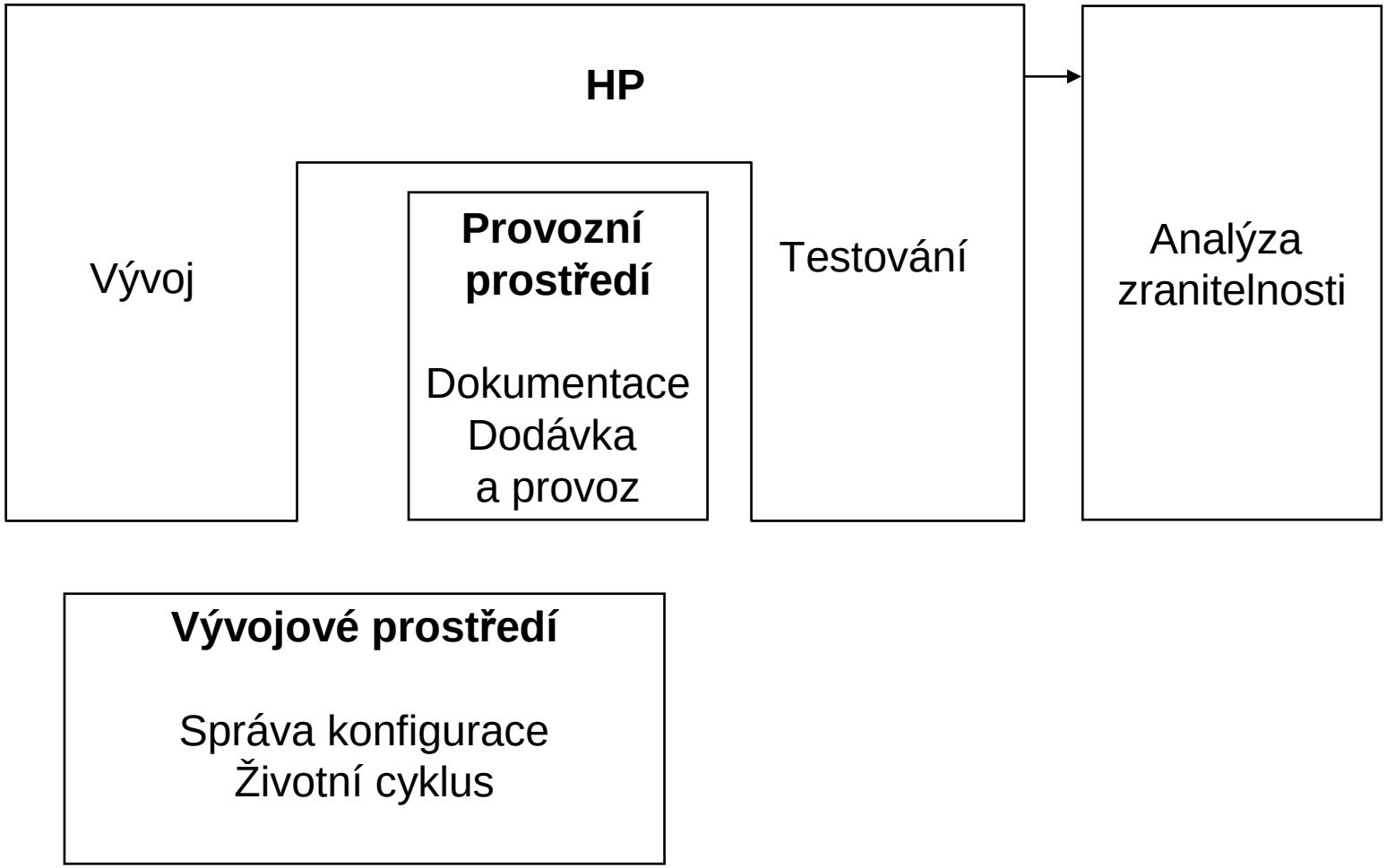
EAL

- **EAL1 - (nová)**
  - Nejnižší úroveň pro hodnocení
- **EAL2 - (odpovídá C1 - E1)**
  - Nejlepší, čeho lze dosáhnout bez dodatečné práce vývojáře
- **EAL3 - (odpovídá C2 - E2)**
  - Dovoluje uvědomělému vývojáři získat bezpečný návrh bez zavažných změn vývojových postupů
- **EAL4 - (odpovídá B1 - E3)**
  - Nejlepší, čeho lze dosáhnout bez zavažných změn vývojových postupů
- **EAL5 - (odpovídá B2 - E4)**
  - Nejlepší, čeho lze dosáhnout pomocí plánovaného a kvalitního vývoje bez extrémně vysokých nákladů
- **EAL6 - (odpovídá B3 - E5)**
  - “high tech” úroveň pro typicky vojenské použití
- **EAL7 - (A1 - E6)**
  - Nejvyšší dosažitelná bezpečnost, hranice současné technologie

Třídy požadavků zaručitelnosti

- **ACM: Správa konfigurace**
  - Automatizace správy konfigurace, Akceptační procedury
- **ADO: Dodávka a provoz**
  - Detekce modifikace, Procedury pro instalaci, generování a start
- **AGD: Dokumentace**
  - Dokumentace pro uživatele a správce
- **ALC: Podpora životního cyklu**
  - Definovaný model životního cyklu, Definované vývojové nástroje
- **AVA: Analýza zranitelnosti**
  - Analýza síly bezpečnostních funkcí, Nezávislá analýza zranitelnosti
- **ADV: Vývoj**
  - Model Bezpečnostní politiky, Funkční specifikace, Model architektury, Detailní model, Důkaz korespondence
- **ATE: Testování**
  - Testování podle Funkční specifikace, Modelu architektury, Analýza pokrytí testů

Uplatnění tříd záruky



Úroveň záruky EAL 4

- Podle definice "metodicky navrhovaný, testovaný a přezkoumávaný produkt nebo systém IT"
- Umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti, založenou na dobrých komerčních vývojových praktikách, které nepožadují mimořádně velké odborné znalosti, dovednosti a jiné zdroje
- Používá některé formální postupy
- Nejvyšší úroveň pro běžně vyráběné produkty

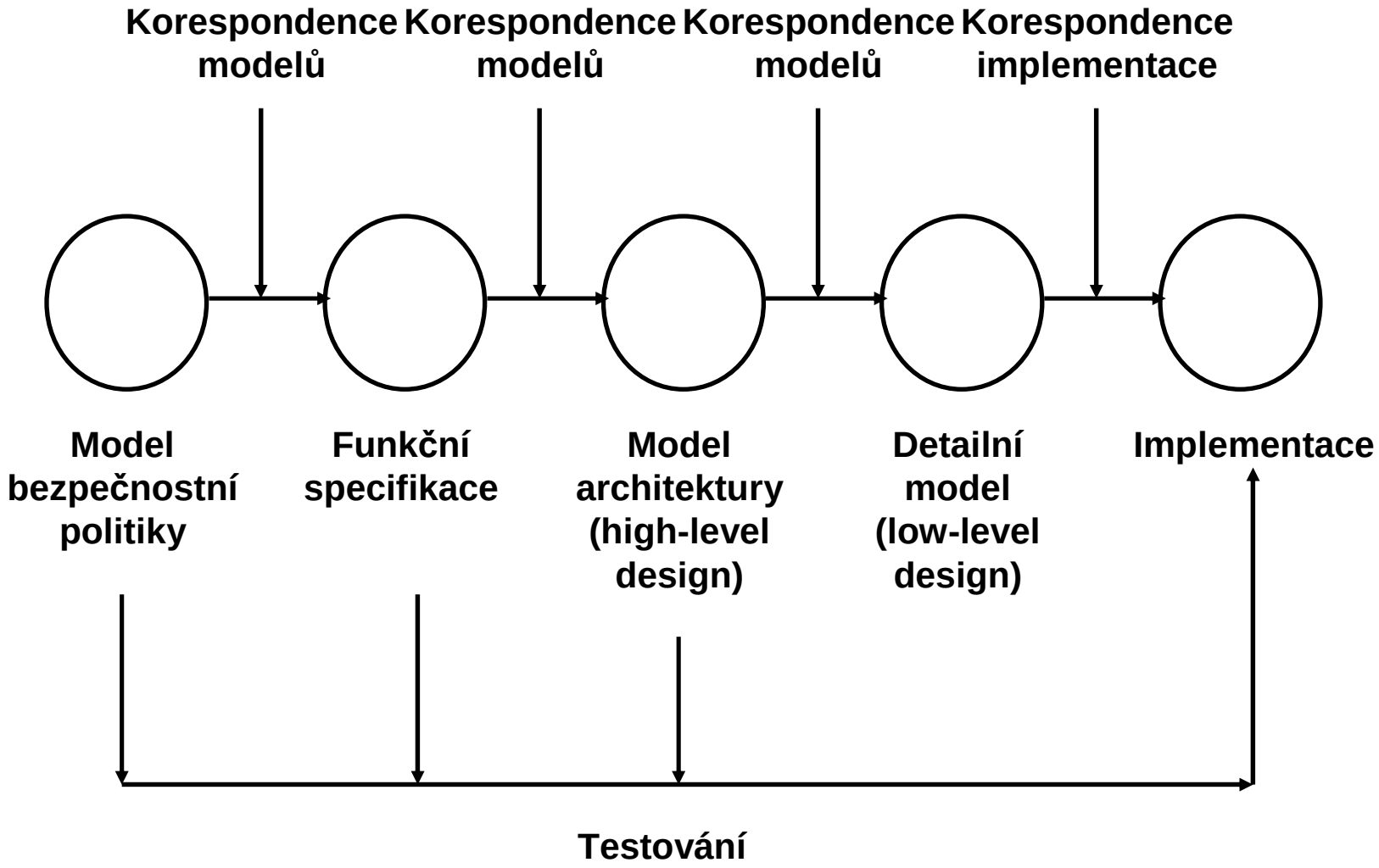
Neformální, poloformální, formální

- **Neformální model/specifikace**
  - zapsána v přirozeném jazyce
  - nepodléhá žádným speciálním omezením
- **Poloformální model/specifikace**
  - vyžaduje užití některé omezující notace (nebo notací) spolu s množinou konvencí
  - může mít buď grafickou podobu, nebo může být založen na omezeném užití přirozeného jazyka
  - např. grafy toku dat, diagramy vzájemných vztahů mezi entitami a relacemi, grafy datových struktur, grafy struktury procesu nebo programu, notace SDL doporučená CCITT.
- **Formální model/specifikace**
  - zapsána ve formální notaci, která využívá dobře definovaných matematických pojmů
  - např. metoda VDM, Z notace, RAISE Specification Language, Gypsy Specification Language, ISO Protocol Specification Language

Jednotlivé modely při vývoji

- **Model bezpečnostní politiky**
  - **popisuje komponenty bezpečnostní politiky, které jsou zabezpečeny bezpečnostními funkcemi**
- **Funkční specifikace**
  - **popis bezpečnostních funkcí a externích rozhraní**
- **Model architektury (high-level design)**
  - **popis posloupnosti akcí, které jsou provedeny v každém subsystému na základě stimulu na jeho rozhraní**
- **Detailní model (low-level design)**
  - **popis realizace posloupnosti akcí, které jsou provedeny v každém subsystému na základě stimulu na jeho rozhraní**
  - **musí obsahovat všechny identifikovatelné komponenty (např. funkce, procedury atd.)**
- **Implementace**

Vývoj


Korespondence modelů
Korespondence modelů
Korespondence modelů
Korespondence implementace
Model bezpečnostní politiky
Funkční specifikace
Model architektury (high-level design)
Detailní model (low-level design)
Implementace
Testování

CEM - Common Evaluation Methodology

- Doplněk k CC
- Popisuje aktivity hodnotitele
- Důležitá pro vzájemné uznávání
- Část 1: Úvod a obecný model
  - Terminologie a principy hodnocení
- Část 2: Metodologie hodnocení
  - PO a BC
  - EAL 1-4
  - EAL 5-7
- Část 3: Rozšíření metodologie

Management bezpečnosti

Celková bezpečnostní politika (CBP)

- **Globální popis cílů organizace, jejího IS a zabezpečení**
- **Cíl**
  - **ochrana majetku, pověsti a činnosti instituce**
- **Dokument**
  - **nadčasový, nezávislý na použité technologii, (horizont 5-10 let)**
  - **přijatý vedením organizace jako vnitroinstitucionální norma**
  - **závazný dokument, veřejný dokument**
- **Stanovuje**
  - **citlivé informace, ostatní citlivá aktiva a jejich klasifikaci**
  - **jednoznačné (hierarchické) zodpovědnosti & práva & pravomoci**
  - **minimální sílu použitých bezpečnostních mechanismů**
- **Stručný a srozumitelný, úplný dokument**
  - **otázky a konflikty lze vyřešit odkazem na paragrafy CBP**

Příklad struktury CBP

- Popis organizace, jejího poslání a koncepcí IT organizace
- Rámcový plán a harmonogram vybudování celkové bezpečnostní politiky
- Cíle CBP
- Specifikace potřebné struktury zodpovědnosti a pravomocí
- Identifikace (kritických) aktiv, zvláště pak citlivých dat
- Identifikace obecných hrozeb
- Výsledky orientační analýzy rizik
- Popis stávajícího stavu zabezpečení
- Doporučení, jak dosáhnout bezpečnostních cílů
- Cíle a strategie havarijních plánů
- Omezení respektovaná bezpečnostní politikou
    - návaznosti na relevantní zákony, vyhlášky a předpisy
- Časové plány implementace a pravidelných akcí, revizí/oprav
- Návrh a koncepce programu školení a osvěty

Systémová bezpečnostní politika (SBP)

- **Systémová bezpečnostní politika**
  - **Definuje způsob implementace celkové bezpečnostní politiky IT v konkrétním prostředí**
  - **Stanovuje soubor principů a pravidel pro ochranu IS**
  - **Zabývá se volbou konkrétních technických, procedurálních, logických a administrativních bezpečnostních opatření**
  - **Částečně i volbou fyzických a personálních bezpečnostních opatření, pokud tyto mohou ovlivnit bezpečnost IS**
  - **Implicitně se zabývá bezpečností elektronické (počítačové) části IS**
  - **Pokud je IS příliš rozsáhlý a různorodý, je vhodné vypracovat samostatně systémovou bezpečnostní politiku pro různé oblasti nebo subsystémy**

Tvorba bezpečnostní politiky

- **BP nikdy nevzniká jednorázovou akcí**
- **životní cyklus tvorby BP lze zjednodušeně vyjádřit následujícími (opakovaně) prováděnými kroky**
  - **1. posouzení vstupních vlivů**
  - **2. analýza rizik**
  - **3. vypracování BP**
  - **4. implementace BP**
  - **5. nasazení BP, kontrola její účinnosti a vyslovování závěrů**

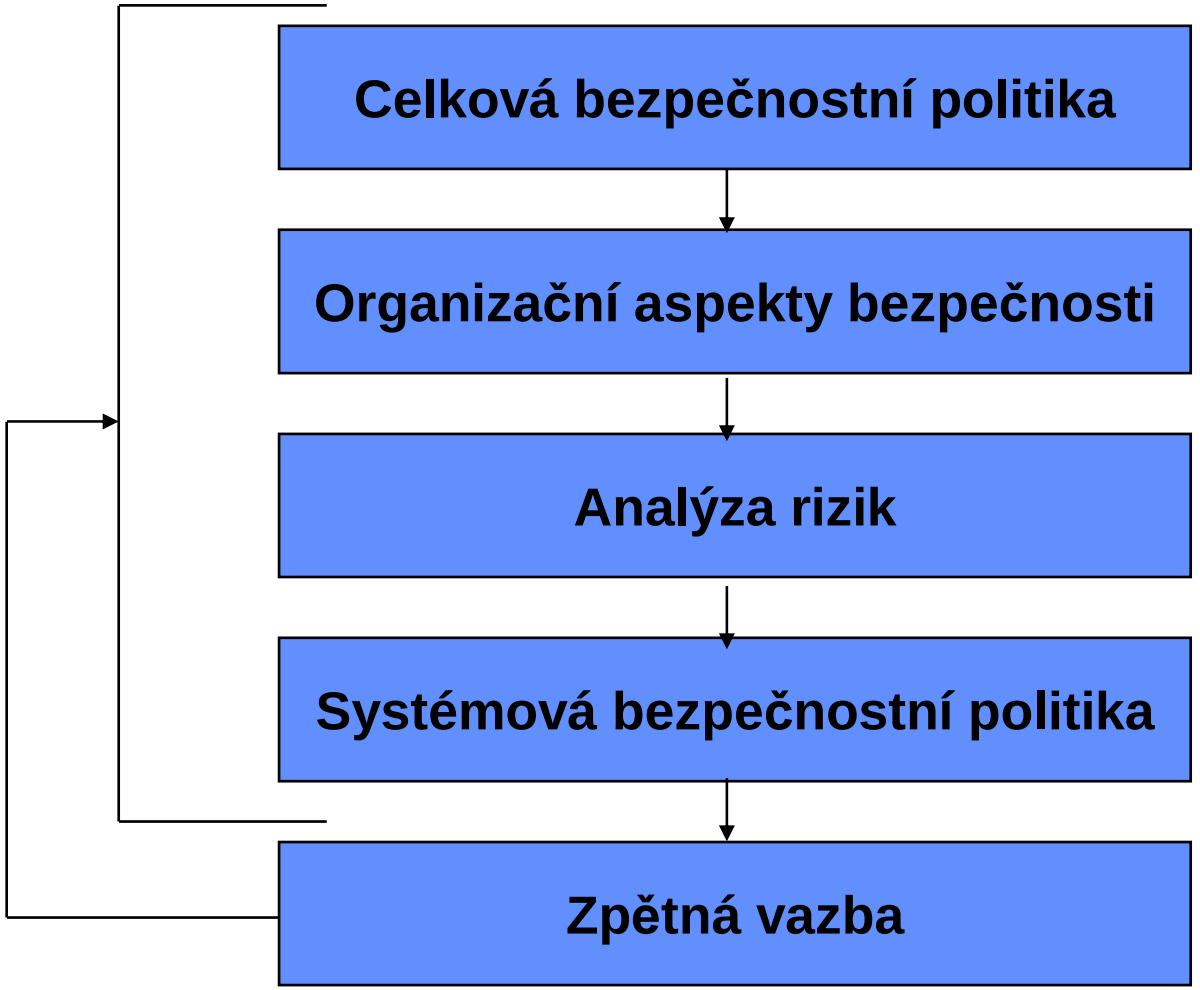
Normy a standardy

- **TR 13335 - Guidelines for the Management of IT Security**
  - **ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3**
- **BS7799 - Code of Practice for Information Security Management**
  - **ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti**
- **ISO 27001**
  - **nová mezinárodní norma pro Systém správy informační bezpečnosti (Information Security Management System, ISMS)**

TR 13335

- **Part 1: Concepts and Models for IT Security**
- **Part 2: Managing and Planning IT Security**
- **Part 3: Techniques for the Management of IT Security**
- **Part 4: Selection of Safeguards**
- **Part 5: Safeguards for External Connections**

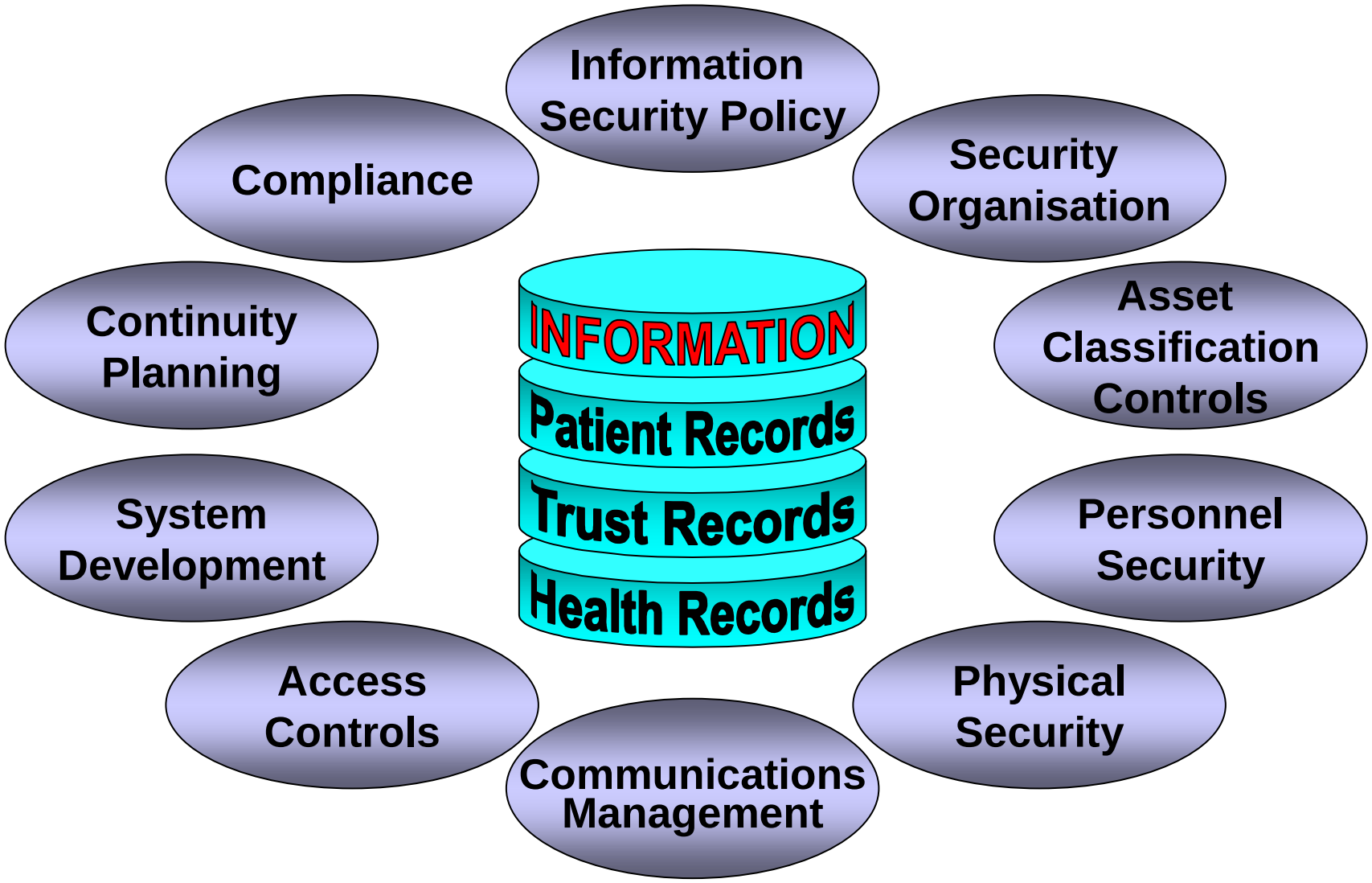
TR 13335 - Proces bezpečnosti IT



BS7799 - Code of Practice for Information Security Management

- Britský standard, který je používán i v jiných evropských zemích
- Určen jako referenční dokument pro osoby zodpovědné za implemementaci a udržování informační bezpečnosti v organizaci
- Certifikační schéma, zvané c:cure, podobné ISO 9000
- Přijato jako norma ISO/IEC 17799:2000
  - ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti
- 1. ISO 17799 definuje 10 řídicích principů
- 2. BS 7799-2:1999 obsahuje:
  - 36 cílů
  - 127 opatření

Principy BS 7799

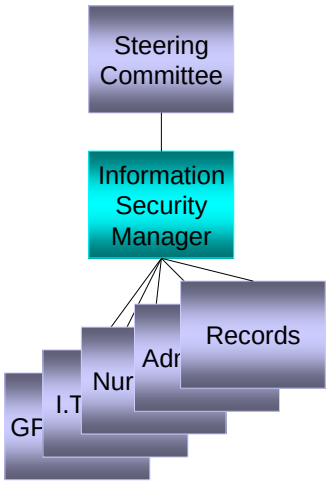


Bezpečnostní politika

- **Určuje směr zabezpečení a zajišťuje manažerskou podporu**
  - **Existence BP v organizaci**
  - **Správa a aktualizace BP**

Organizace bezpečnosti

- **Správa bezpečnosti v organizaci**
- **Bezpečnostní infrastruktura**
  - **Definice rolí, povinností a odpovědností**
  - **Koordinace**
  - **Allocation of information security responsibilities**
- **Outsourcing**



Klasifikace a správa aktiv

- **Klasifikace hodnoty a kritičnosti aktiv**
- **“Kritická aktiva“**

Personální bezpečnost

- **Je namířena přímo na osoby (nikoli prostřednictvím IS)**
- **Je převážně preventivní**
- **Je založena na**
  - » **důvěryhodnosti pracovníka**
  - » **spolehlivosti pracovníka**

Fyzická bezpečnost

- Fyzická bezp. opatření fyzickým způsobem omezují přístup ke komponentám informačního systému
- Zabraňují hrozbám pro fyzické komponenty systému

Komunikace a provoz

- Především administrativní bezpečnostní opatření
- Bezpečnostní procedury, prováděné lidmi

Řízení přístupu

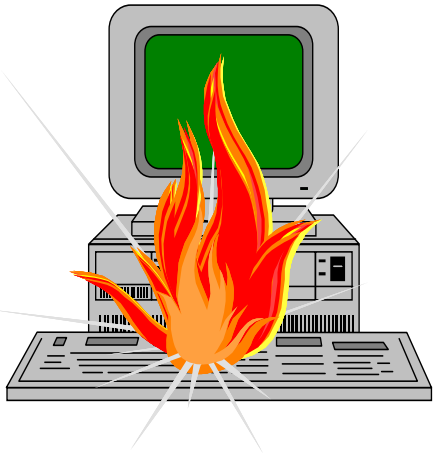
- **Povolit pouze oprávněný přístup k informacím, službám a dalším prostředkům**
  - **Ochrana před ztrátou, prozrazením, modifikací nebo podvržení informací**

Vývoj a údržba systému

- **Zajištění bezpečnosti životního cyklu systému**

Zajištění kontinuity

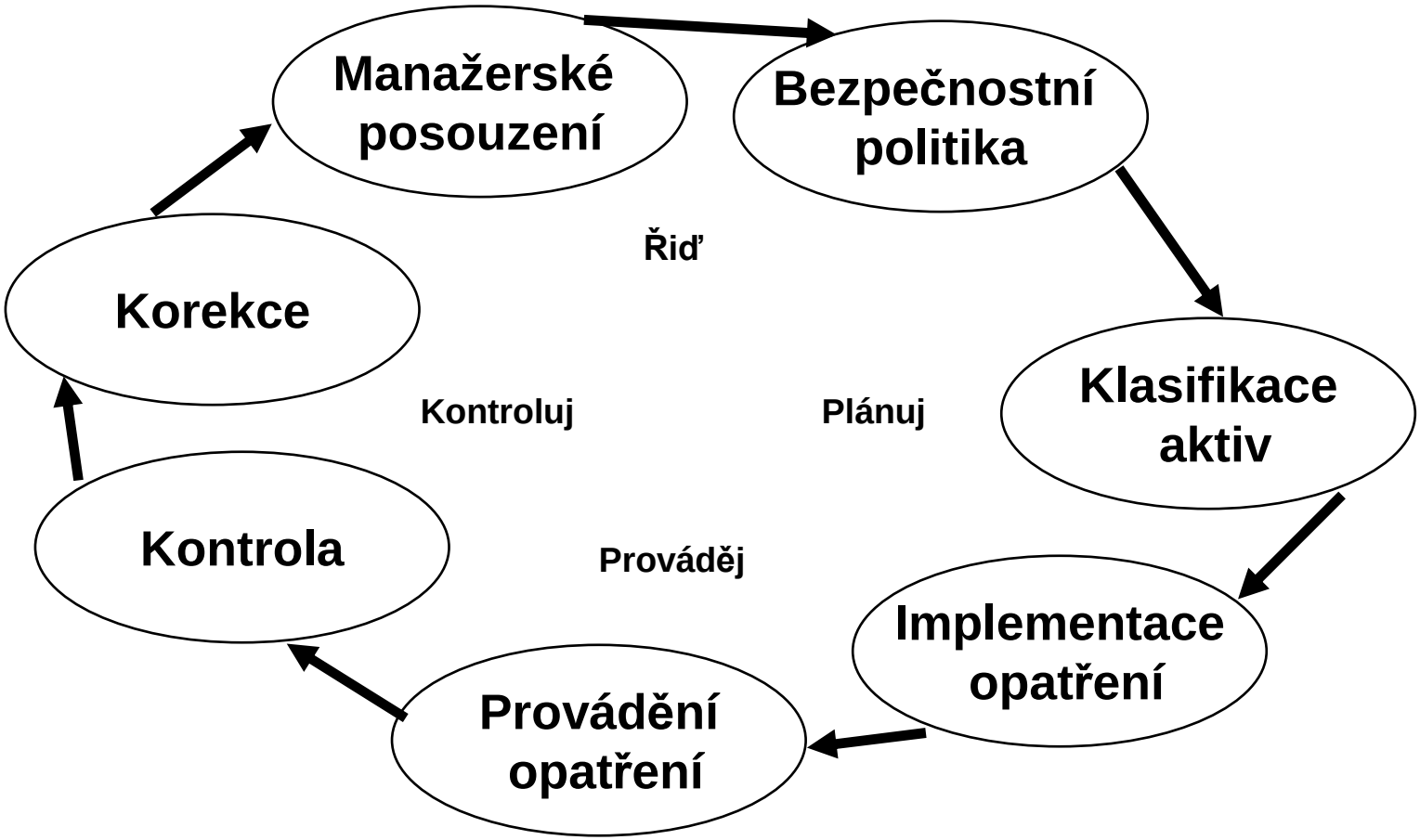
- **Cíl: zabránit přerušení obchodních aktivit a ochránit kritické procesy před výpadky**
- **Havarijní plány**



Shoda

- **Jde především o shodu se zákony a jinými normami**

Implementace BS 7799



ISO 27001

- **ISO 27001 je nová mezinárodní norma pro Systém správy informační bezpečnosti (Information Security Management System, ISMS)**
- **Postupně nahradí BS7799-2**
  - **Specifikuje požadavky na zavedení ISMS**
- **ISO 27001 je první normou v nové sérii mezinárodních norem pro správu bezpečnosti**
- **Je harmonizována s:**
  - **ISO9001:2000 (Quality Management System)**
  - **ISO14001:1996 (Environmental Management System)**

ISO 27001 - Oblasti

- **Security policy**
  - **Bezpečnostní politika**
- **Organisation of information security**
  - **Organizace informační bezpečnosti**
- **Asset management**
  - **Správa aktiv**
- **Human resources security**
  - **Personální bezpečnost**
- **Physical and environmental security**
  - **Fyzická bezpečnost**
- **Communications and operations management**
  - **Bezpečnost komunikací a provozu**

ISO 27001 - Oblasti

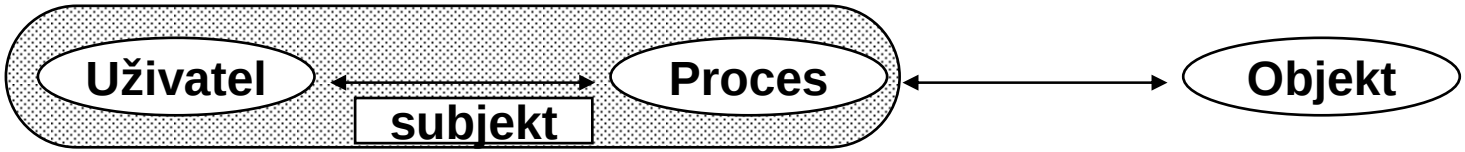
- **Access control**
  - **Řízení přístupu**
- **Information systems acquisition, development and maintenance**
  - **Pořizování, vývoj a údržba**
- **Information security incident management**
  - **Správa bezpečnostních incidentů**
- **Business continuity management**
  - **Správa kontinuity**
- **Compliance**
  - **Shoda**

Modely bezpečnosti

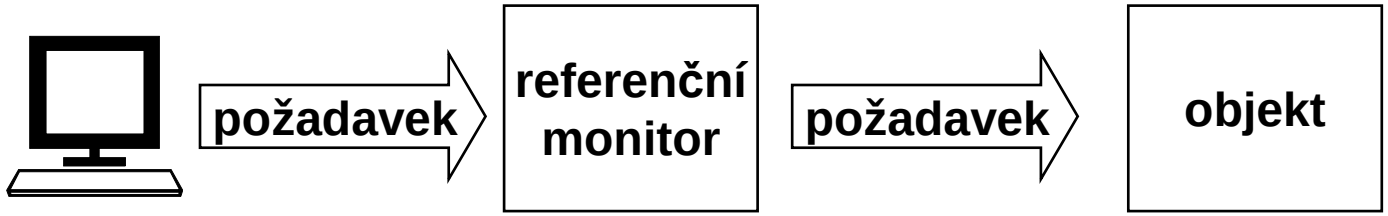
Modely bezpečnosti

Formální vyjádření části bezpečnostní politiky

- **podle řízení přístupu**
  - **povinné řízení přístupu**
  - **nepovinné řízení přístupu**
- **podle klasifikace informace**
  - **jednoúrovňové X víceúrovňové**
- **podle cílů, které zajišťují**
  - **modely důvěrnosti**
  - **modely integrity**
  - **modely dostupnosti**
- **entity**
  - **uživatel, proces, objekt, subjekt**



Monitor



- **Definován v Orange Book**
- **Prostředek pro lokalizaci bezpečnostních funkcí do jednoho místa**
- **Požadavky**
  - **nelze jej obejít**
  - **je odolný proti útoku (schopen zajistit vlastní integritu)**
  - **malý, aby mohl být podroben analýze správnosti**

Víceúrovňové modely

- **Stupeň utajení**

  neklasifikovaná < důvěrná < tajná < přísně tajná

- **Kategorie**

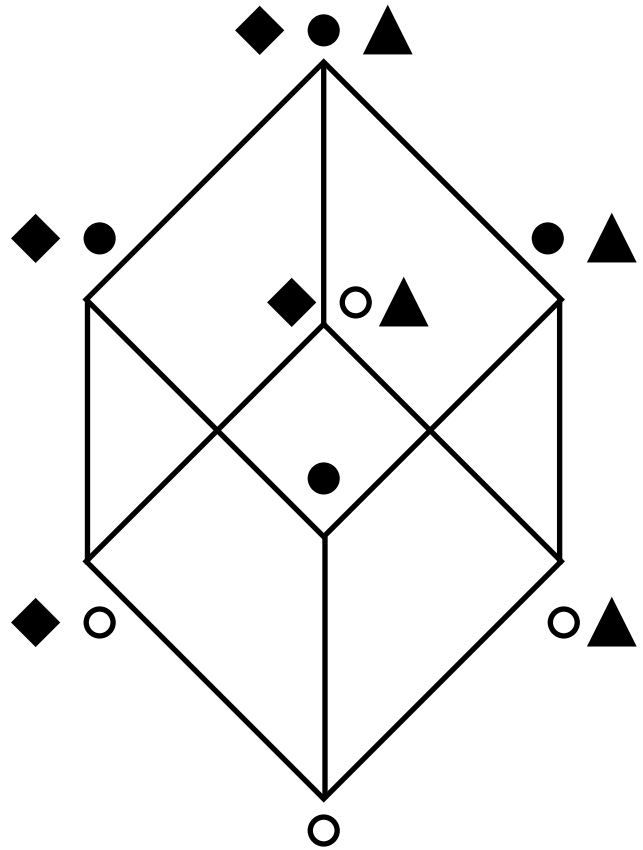
  osobní, obchodní, ...

- **Bezpečnostní atributy**

  <stupeň utajení, kategorie>

- **Relace <=**
  - **O<=S jen tehdy, pokud**
    stupeň-utajení$_O$ <= stupeň-utajení$_S$ a
    kategorie$_O$ $\subseteq$ kategorie$_S$

Svazový model pro více úrovní

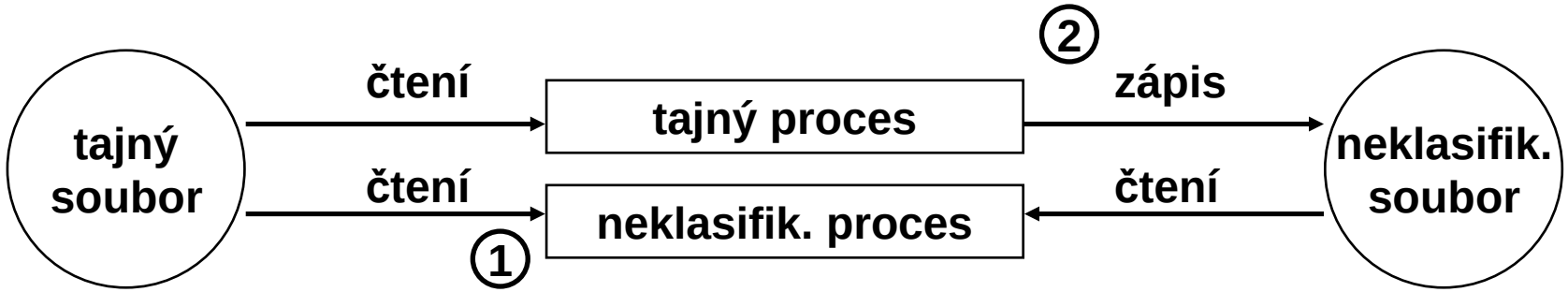


neklasifikované
osobní
tajné
obchodní

- **transitivita**
  - **if a<=b and b<=c then a<=c**
- **antisymetrie**
  - **if a<=b and b<=a then a=b**
- **nejvyšší prvek**
  - **<tajné, {osobní, obchodní}>**
- **nejnižší prvek**
  - **<neklasifikované, {}>**
- **některé prvky jsou neporovnatelné**
  - **<tajné, osobní>**
    <tajné, obchodní>

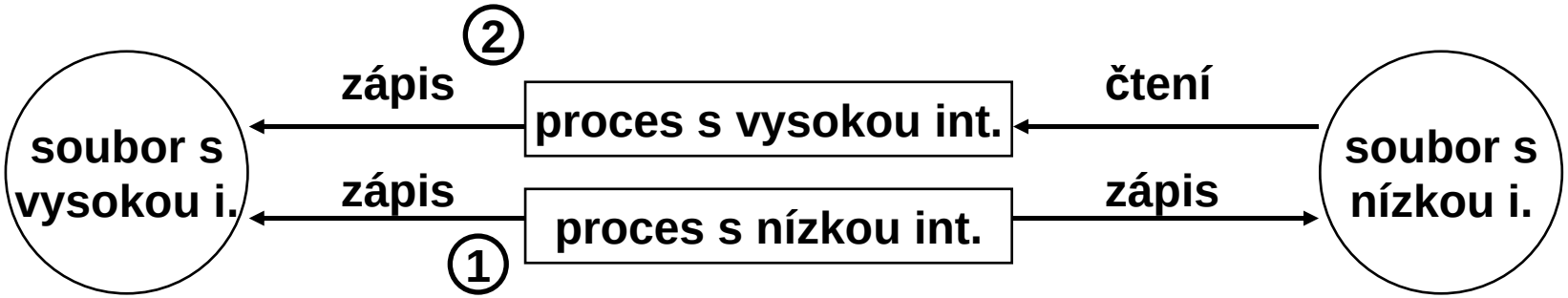
Bell-LaPadulův model důvěrnosti

- **Ohodnocení subjektu a objektu**
  - **stupeň důvěry v subjekt *C(s)***
  - **úroveň důvěrnosti objektu *C(o)***
- **Jednoduchá ochrana (1)**
  - **subjekt *s* může číst objekt *o*, pokud**
    C(s) >= C(o)
- **Omezující vlastnost (*-vlastnost) (2)**
  - **pokud subjekt *s* může číst objekt *o*, pak může modifikovat objekt *p*, pokud *C(p) >= C(o)***

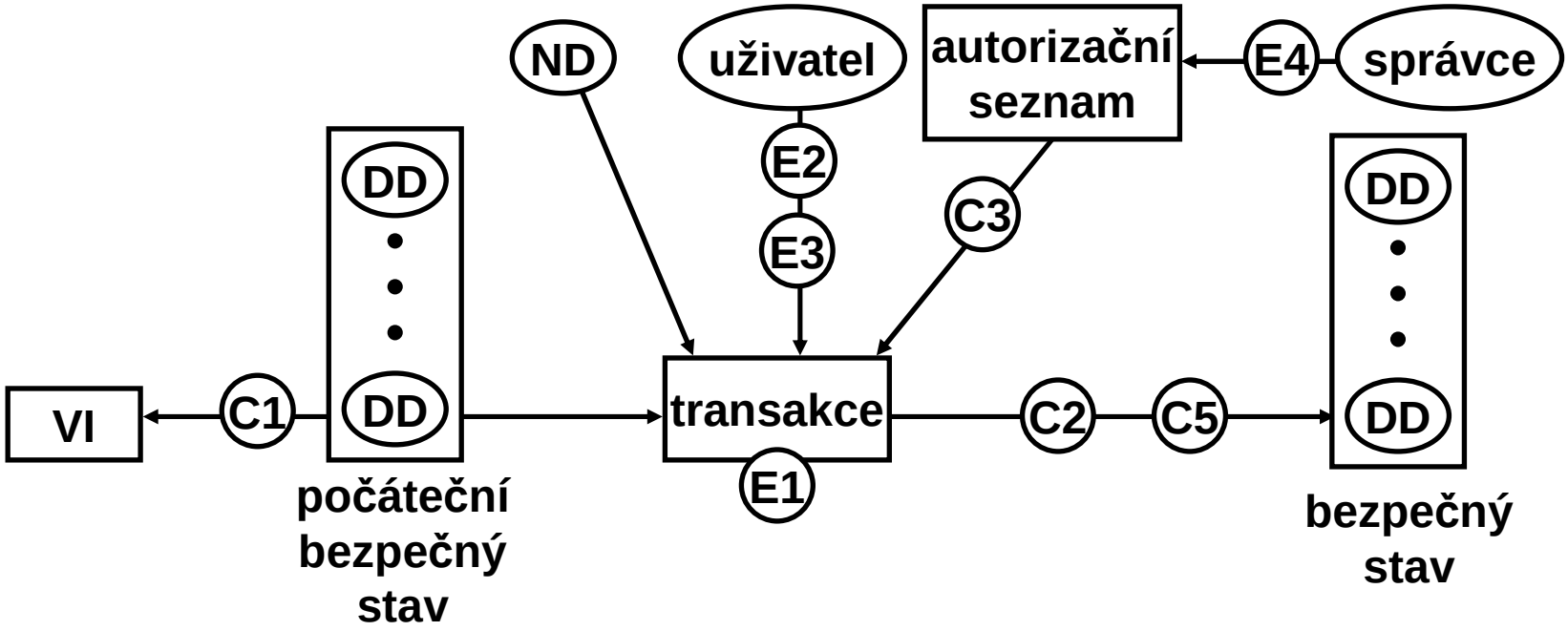


Bibův model integrity

- **Je duálním modelem k Bell-LaPadulovu modelu**
  - **stupeň důvěry v subjekt *I(s)***
  - **úroveň integrity objektu *I(o)***
- **Jednoduchá ochrana (1)**
  - **subjekt *s* může modifikovat objekt *o*, pokud**
    I(s) >= I(o)
- **Omezující vlastnost (*-vlastnost) (2)**
  - **pokud subjekt *s* může číst objekt *o*, pak může modifikovat objekt *p*, pokud *I(o) >= I(p)***



Clark-Wilsonův model integrity



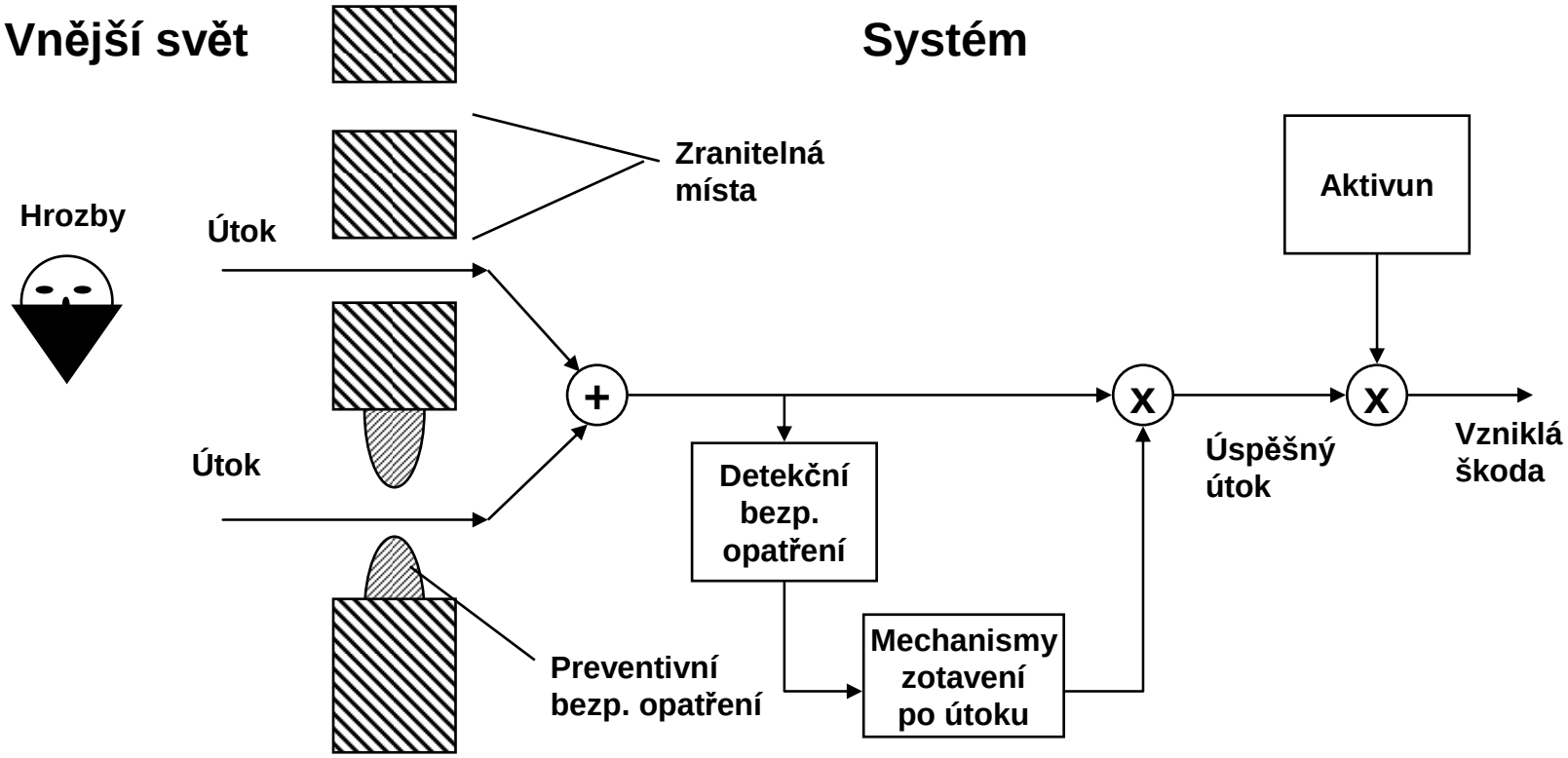
- DD - důvěryhodná data
- ND - nedůvěryhodná data
- VI - verifikace integrity
- E1 - DD je měněno autorizovanou transakcí
- E2 - uživatel je autentizován
- E3 - uživatel je autorizován
- E4 - autorizaci mění pouze správce
- C1 - VI zkontroluje, že DD jsou bezpečná
- C2 - TP zachovává bezpečnost dat
- C3 - oddělení pravomocí
- C4 - transakce změní ND na DD

Modely dostupnosti

- **Systém kvót**
  - **každý uživatel má omezeno množství prostředků, které mu lze přidělit**
    - » **prostor na disku, prostor v paměti, čas procesoru, délka relace, počet tiskových stran....**
- **Amorosův model**
  - **každý uživatel má prioritu *p* a prostředek kritičnost *c***
  - **funkce *prevent(p,c)* říká, zda se má prostředek uživateli poskytnout**
- **Yu-Gligorův model**
  - **spravedlnost - uživatel nebude blokován navždy, pokud je možnost, aby pokračoval**
  - **simultánnost - uživatel někdy dostane všechny možnosti, jak pokračovat**
  - **dohoda uživatelů - současné požadavky uživatelů na službu jsou uspořádány podle analýzy všech ostatních požadavků**

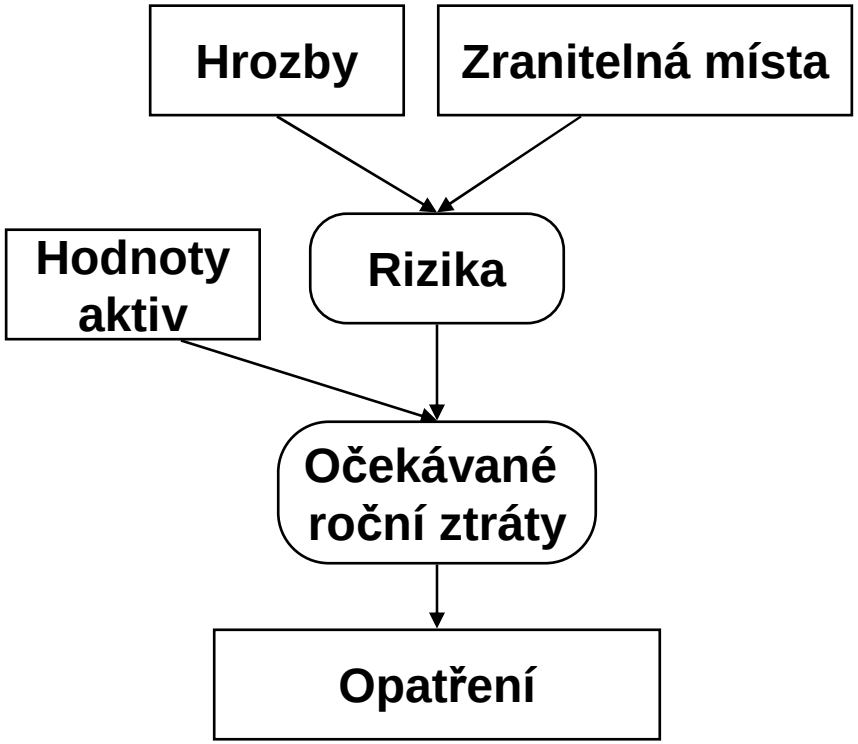
Analýza rizik

Model incidentu



Proces analýzy rizik

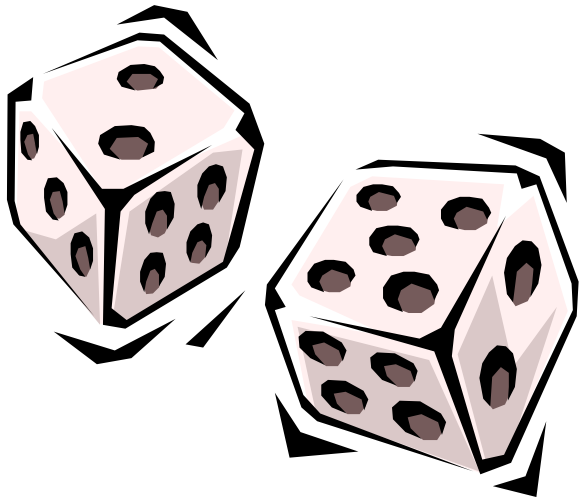
- **Identifikace aktiv**
- **Stanovení zranitelných míst a hrozeb**
- **Stanovení rizik**
- **Výpočet očekávané roční ztráty (ALE, Annual Loss Expectations)**
- **Volba bezpečnostních opatření**
- *Určení ročních úspor*



Výpočet ALE

- **Riziko**
  - **škodlivý efekt uskutečnění hrozby**
  - **škodlivý efekt využití zranitelného místa**
- **Riziko závisí na :**
  - **P - pravděpodobnost výskytu bezpečnostního incidentu (např. v jednotkách výskytů za rok)**
  - **C - průměrná škoda vzniklá tímto incidentem**
- **Riziko se vypočte jako**

$$R = P \,.\, C$$



- **Příklad: Organizace má problémy s neoprávněným přístupem k počítačové síti. Panuje obava, že útočník může získat přístup k důvěrným informacím nebo neoprávněně používat výpočetní prostředky organizace.**
- **Rizika:**
  - **Neautorizovaný přístup k datům**
    - **Pravděpodobnost výskytu události 1/tři roky**
    - **Vzniklá škoda 600 000**
    - **Celkem 200 000**
  - **Neautorizovaný přístup k výpočetním prostředkům**
    - **Pravděpodobnost výskytu události 50/rok**
    - **Vzniklá škoda 6 000**
    - **Celkem 30 000**
  - **ALE 230 000**
- **Efektivnost systému pro řízení přístupu: 90% -207 000**
  - **Cena systému pro řízení přístupu:**
    - **Hardware (50 000, amortizace 5 let) 10 000**
    - **Software (30 000, amortizace 5 let) 6 000**
    - **Roční náklady na údržbu 50 000**
    - **Celková cena 66 000**
  - **ALE (po aplikaci systému pro řízení přístupu)**
    - **230 000 - 207 000 + 66 000 = 89 000**
    - **Roční úspory (230 000 - 89 000) = 141 000**

Generace analýzy rizik

- **1972… Metody „Checklist“**
  - **Výběr z několika řešení na základě dotazníku**
- **1981… Mechanistické inženýrské metody**
  - **Dělení složitých řešení na podúlohy a části**
- **1988… Logické transformační**
  - **Abstrakce problému a řešení**
- **1994… Organizačně řízené**
  - **Hledá se řešení i v netechnických oblastech**

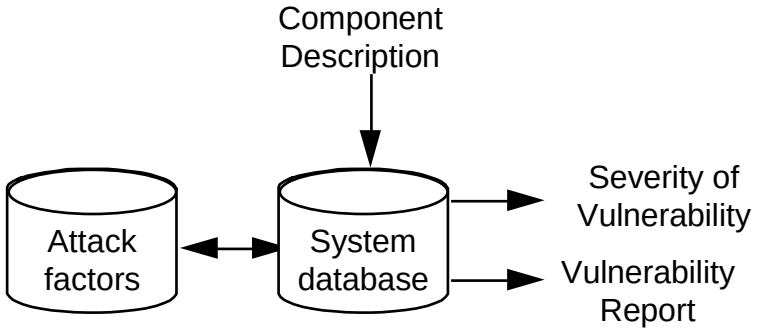
1. Generace

- **Vlastnosti metod první generace**
- **Předpoklady:**
  - **oblast možných řešení je silně omezena**
  - **každé z řešení je značně univerzální**
  - **vliv bezpečnostních opatření je vyjádřen jako snížení pravděpodobnosti výskytu hrozby nebo snížení vlivu hrozby**

VULAN

- **Oblast zranitelnosti**
- **Míra příležitosti útočníka**
- **Míra znalostí útočníka**
- **Čas potřebný pro útok**
- **Vybavení potřebné pro útok**

Výsledkem je zjištěná míra zranitelnosti komponenty.



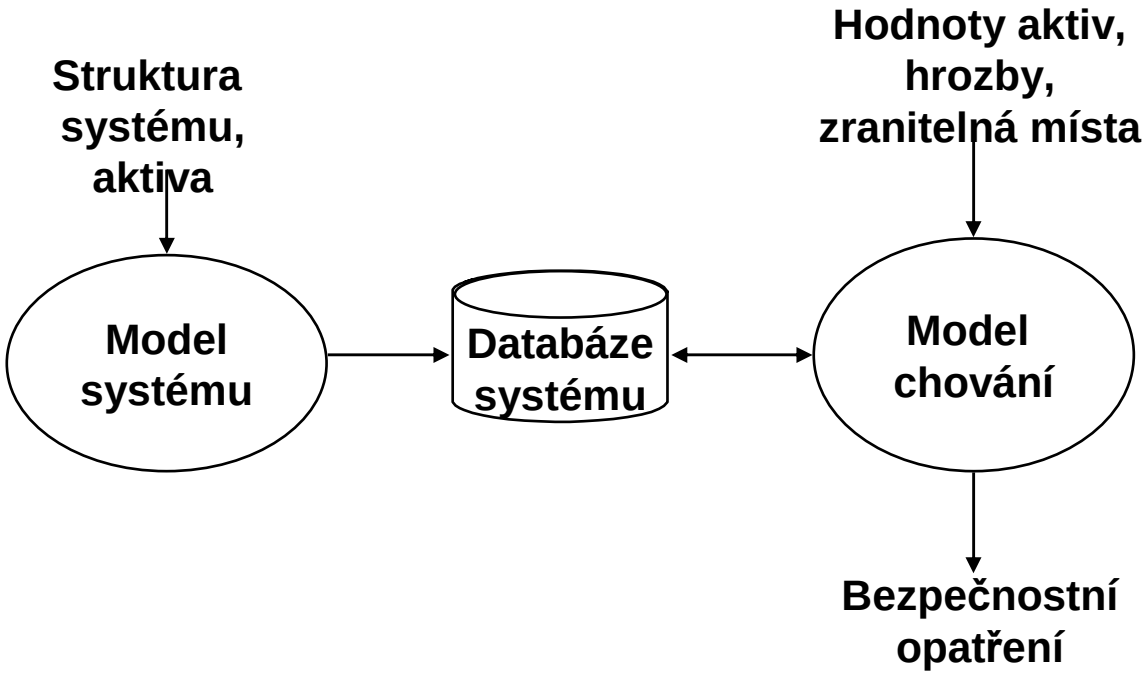

```
                VULNERABILITY REPORT
                                                    Vulner.#: 3
System:  Hardware Security Card 1.0                    Date: 30.04.1995

Vulnerability description:
          Normal user can log-in as any other user,
          normal user can log-in as administrator.

Severity:
Result:   Effective bypassing of logging and acces rights.
Areas:

Cost-equipm: 2,00
Cost-time:   1,00
Knowledge:   3,00
Opportunity: 1,00

                <pomoc:F1><menu:F2><poçítat:Alt-F10>
```

2. Generace

- **Druhá generace - Mechanistické inženýrské metody**
- **Vlastnosti:**
  - **zobrazují problém do velkého množství částečných řešení**
- **Vývojové prostředky:**
  - **návrh shora dolů**
- **Bezpečnostní prostředky:**
  - **Zjišťují odděleně:**
    - » **Aktiva**
    - » **Hrozby**
    - » **Zranitelná místa**

Model analýzy rizik

- **Volbu různých alternativ bezpečnostních opatření může výrazně usnadnit automatizovaný přístup založený na vhodném modelu**
- **Struktura**
  - **Model systému**
  - **Model chování**

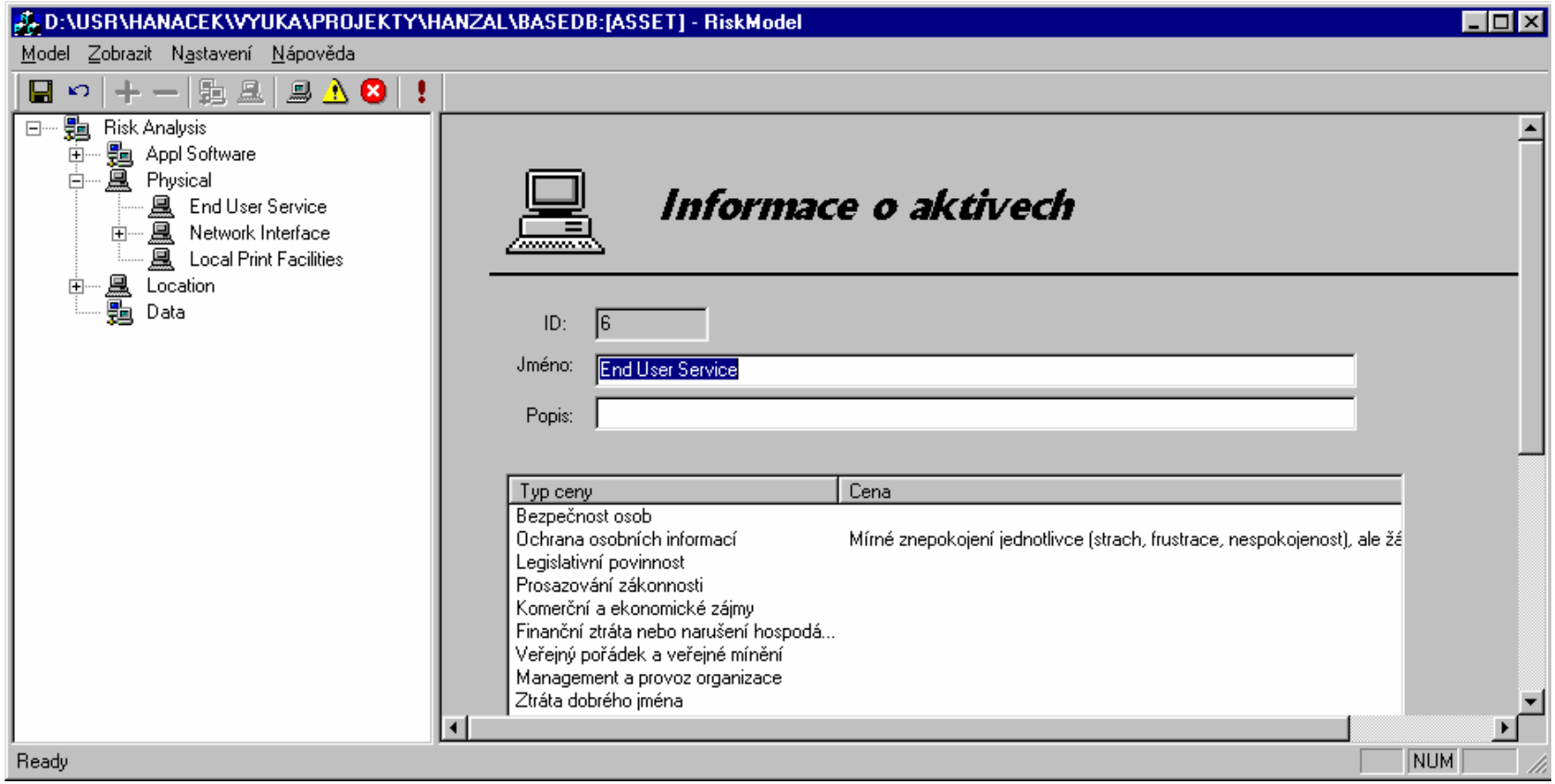


Struktura aktiv

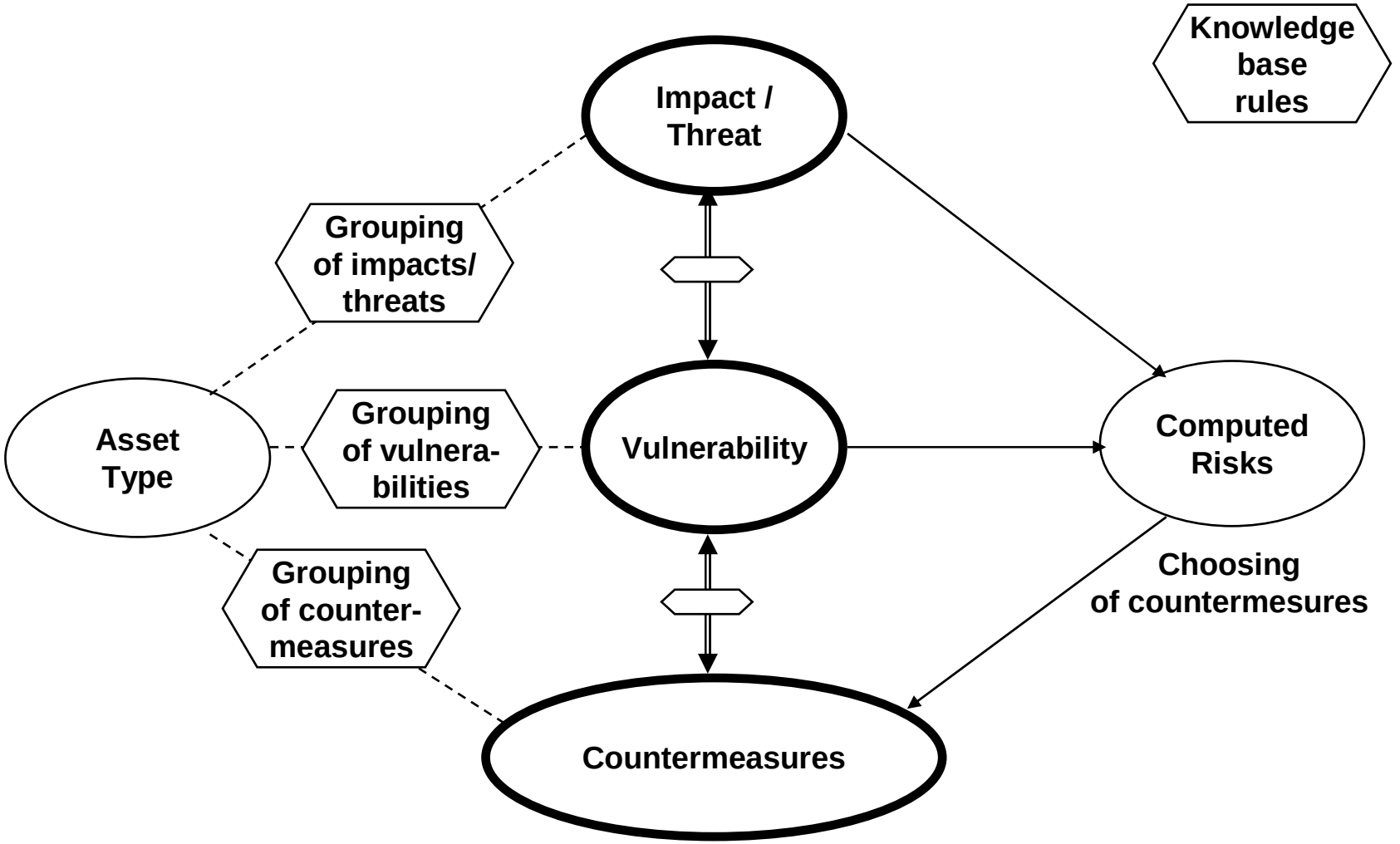
- **Data Asset**
  - **End User Service**
    - **Non-Network Hosts, Network Hosts**
      - **Location**
    - **Non-Network Workstations, Network Workstations**
      - **....**
    - **Local Storage Facility, Network Storage Device**
    - **Local Print Facility, Network Print Server**
    - **Network Distribution Component**
    - **Network Gateway**
    - **Network Management/Operation Host**
    - **Network Interface**
    - **Network Service**
    - **Communications Protocols.**
  - **Application Software**
    - » **Hosts and Workstations**
      - **Location**
  - **Media**
    - » **Location**

Vytváření a ohodnocení aktiv

- **Operace**
  - **Vytváření struktury aktiv a seskupování**
  - **Ohodnocení zranitelných míst a hrozeb**
  - **Export modelu do expertního systému**



Příklad modelu chování



Dotazník pro zjištění hrozeb

Threat : Masquerading of User Identity by Insiders

Threat Questionaire

1 How many attempts have been made by insiders, during the last three years, to gain

unauthorised access to information on the system/network by using another user's account?

Possible Answers

a	None	0
b	Once or twice	10
c	On average once a year	20
d	On average more than once a year	30
e	Unknown	10

2 What is the trend of attempts to gain unauthorised access to the system / network in this

manner?

Possible Answers

a	Increasing	10
b	Remaining constant	0
c	Decreasing	-10

3 Does the system / network hold information which would motivate insiders to gain unauthc

access to the information e.g. personnel files

Possible Answers

a	Yes	5
b	No	0

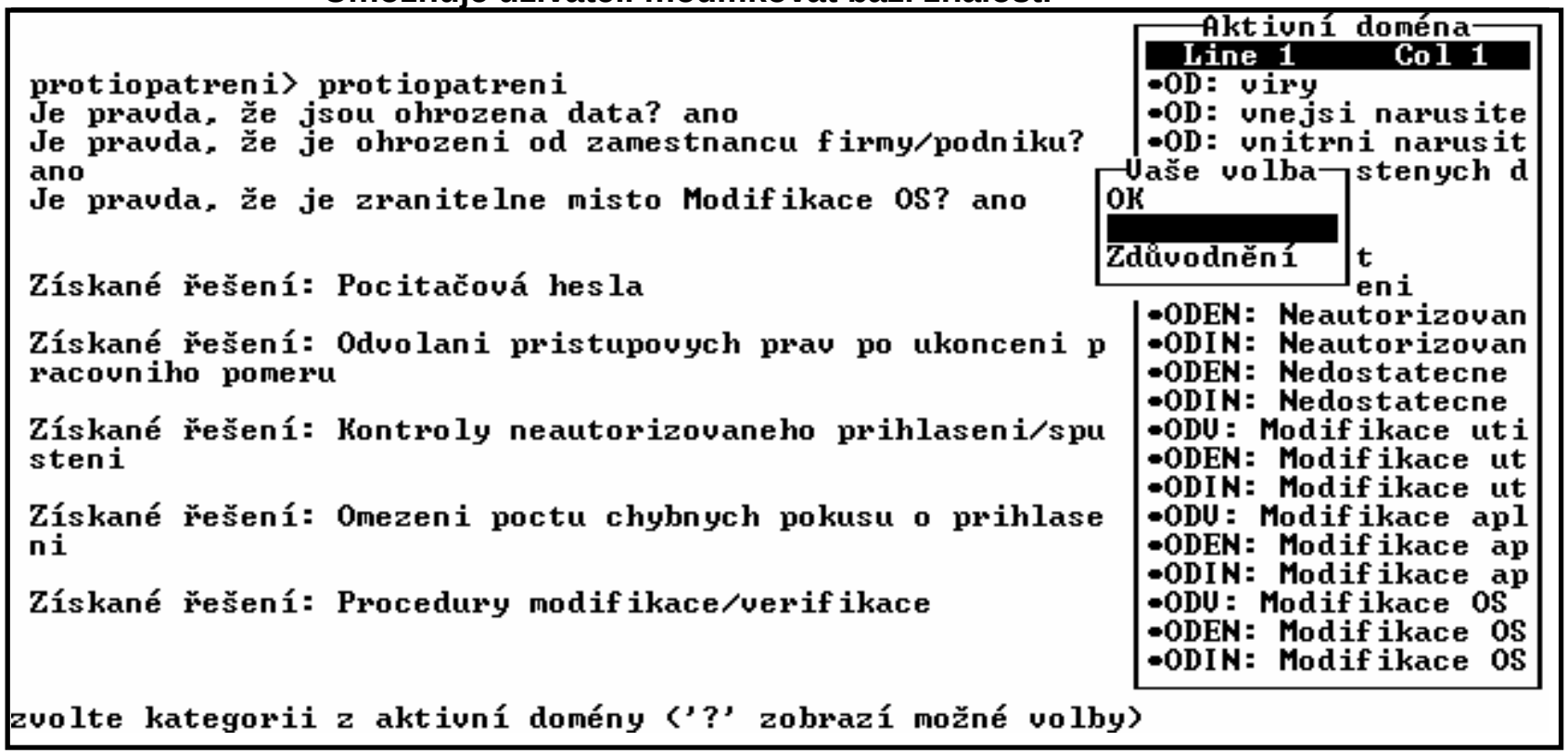
4 Have there been any discovered attempts to subvert insiders by outsiders?

Possible Answers

a	Yes	10
b	No	0

Komunikace s modelem

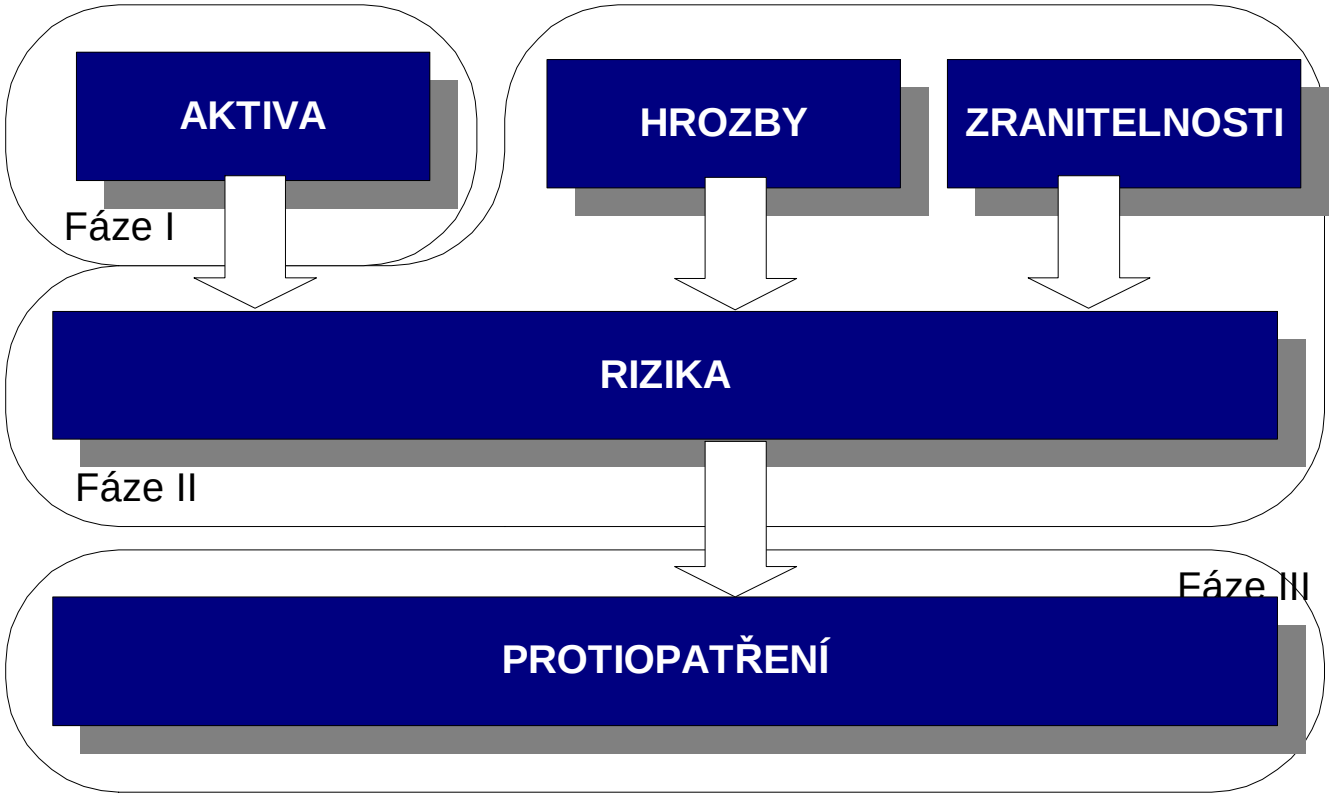
- **Dotazování**
  - Uživatel klade systému dotazy a ten se snaží na základě aktuální báze znalostí odvodit správnou odpověď
- **Prohlížení znalostí**
  - Umožňuje uživateli zobrazit bázi aktuálních znalostí
- **Editace stávající báze znalostí**
  - Umožňuje uživateli modifikovat bázi znalostí



CRAMM

- **Vytvořen původně v roce 1985, stále aktualizován**
- **CRAMM Risk Analysis Methodology je balík, obsahující:**
  - **Správu procesu analýzy rizik**
  - **Související dokumentaci (např. reporty, výsledky a závěry)**
  - **Školení**
  - **Podpůrné softwarové nástroje**

Analýza a řízení rizik pomocí CRAMM



3. Generace

- **Třetí generace - Logicko-transformační metody**
- **Vychází z toho, že model pro analýzu rizik musí znt nejenom strukturu systému, ale i jeho funkčnost**
- **Např. SSADM-CRAMM**

Námitky proti analýze rizik

- **Nepřesná**
  - **Odhady bývají nepřesné a výsledku různých metodologií se často liší**
- **Vyvolává falešný dojem přesnosti**
  - **Špatná interpretace výsledků není chybou metodologie ale chybou uživatele**
- **Neměnnost**
  - **Uživatelé často provedou analýzu rizik jednou a nikdy ji neopakují. Analýza rizik by měla být opakována při každé významné změně vnějších okolností.**
- **Nemá vědecký základ**
  - **Většina metodologií má vědecký základ.**

KONEC