Nároky, požiadavky a kritériá na bezpečný IS

Doc. Ing. Ladislav Hudec, CSc., CISA

Fakulta informatiky a informačných technológií STU

Nezávislý konzultant pre bezpečnosť a ochranu informačných systémov

lhudec@fiit.stuba.sk

Pripravené pre konferenciu ITAPA, Bratislava, hotel Forum, 27.10.2003

Čo je informačná bezpečnosť

Aktívum IS - HW, SW, údaje, obsluha

Bezpečnosť IS spočíva **v udržaní týchto vlastností** IS vo vzťahu k aktívam IS:

- **Dôvernosť**
- **Integrita**
- **Dostupnosť**
- **Účtovateľnosť**

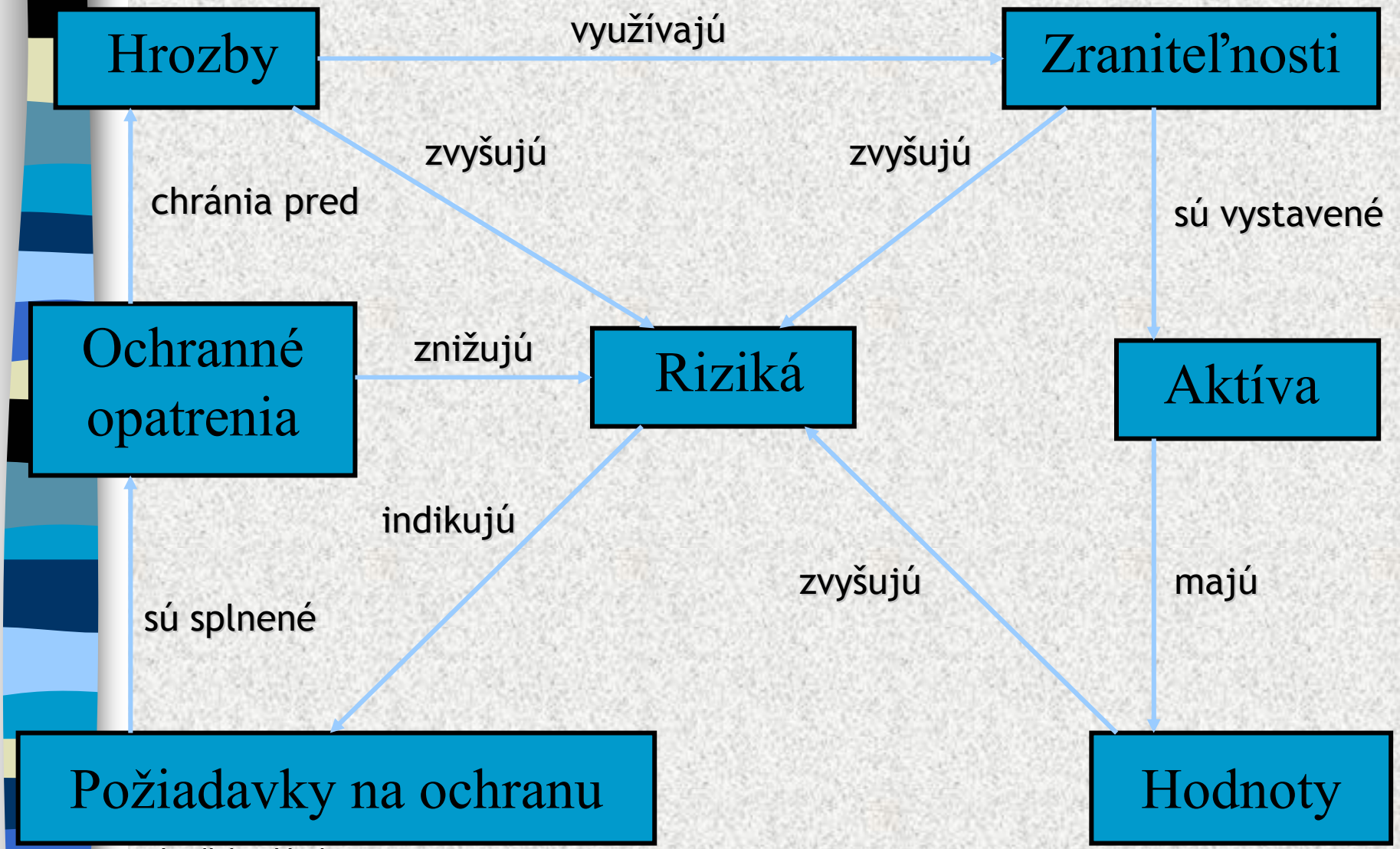
Základné pojmy IB

- **Zraniteľnosť** - zahrňuje slabé miesto aktíva, ktoré môže byť využité hrozbou
- **Hrozba** - akcia alebo potenciálna akcia, ktorá môže porušiť bezpečnosť aktív IS
- **Ochranné opatrenie** - technologické alebo manažérske opatrenie s cieľom redukovania zraniteľnosti a hrozieb
- **Dopad** - strata ako výsledok realizovaných hrozieb (porušenie dôvernosti, modifikácia, falšovanie a nedostupnosť aktív IS, ..)

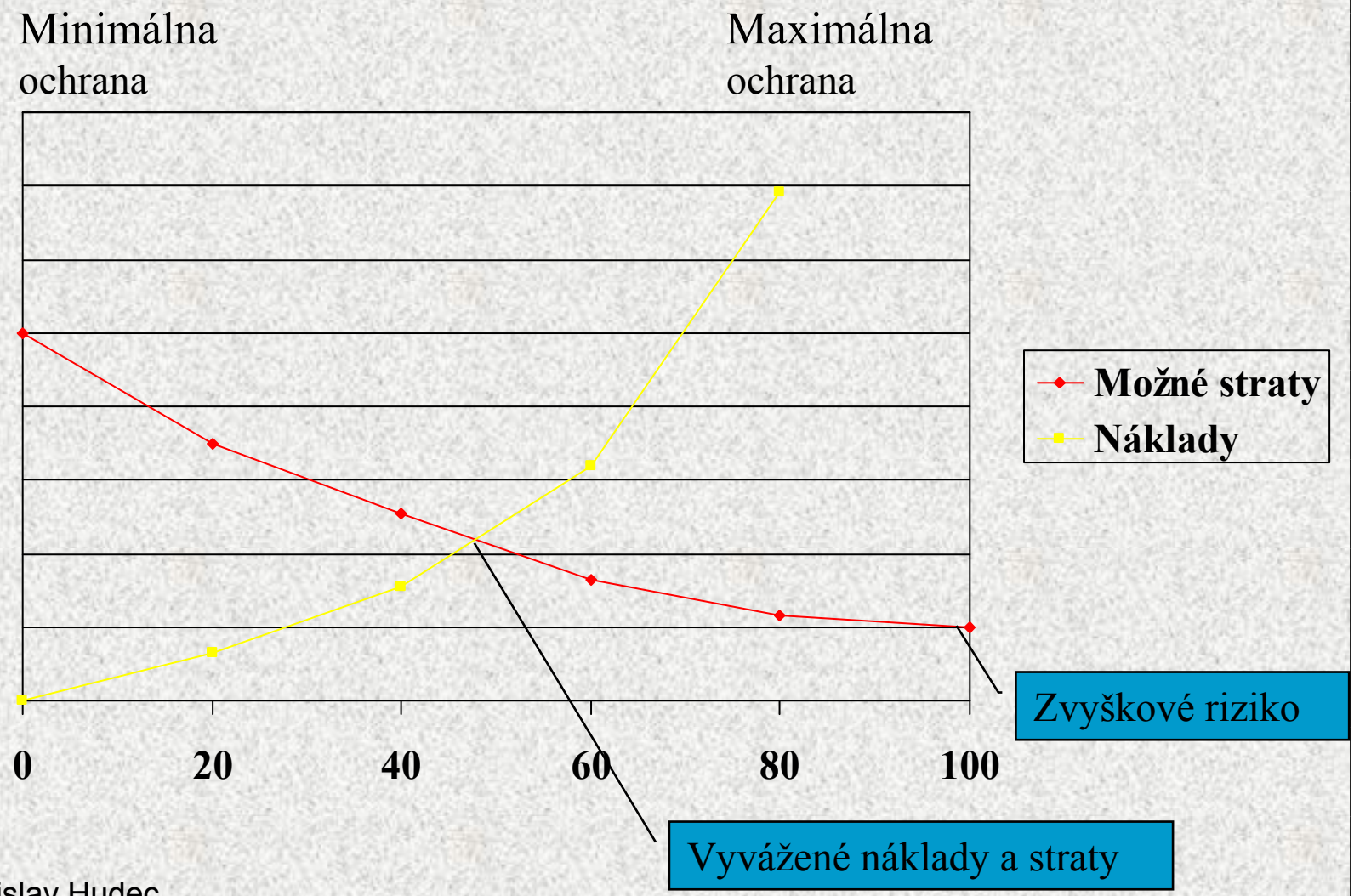
Základné pojmy IB

- **Riziko (bezpečnostné)** - potenciálna možnosť, že daná hrozba využije zraniteľnosť aktív a spôsobí tak stratu alebo zničenie aktív
- **Analýza rizík** - proces identifikovania bezpečnostných rizík, ktorý stanovuje ich závažnosť a identifikuje oblasti vyžadujúce ochranné opatrenie

Vzťahy pri manažmente rizík



Ekonomika bezpečnosti

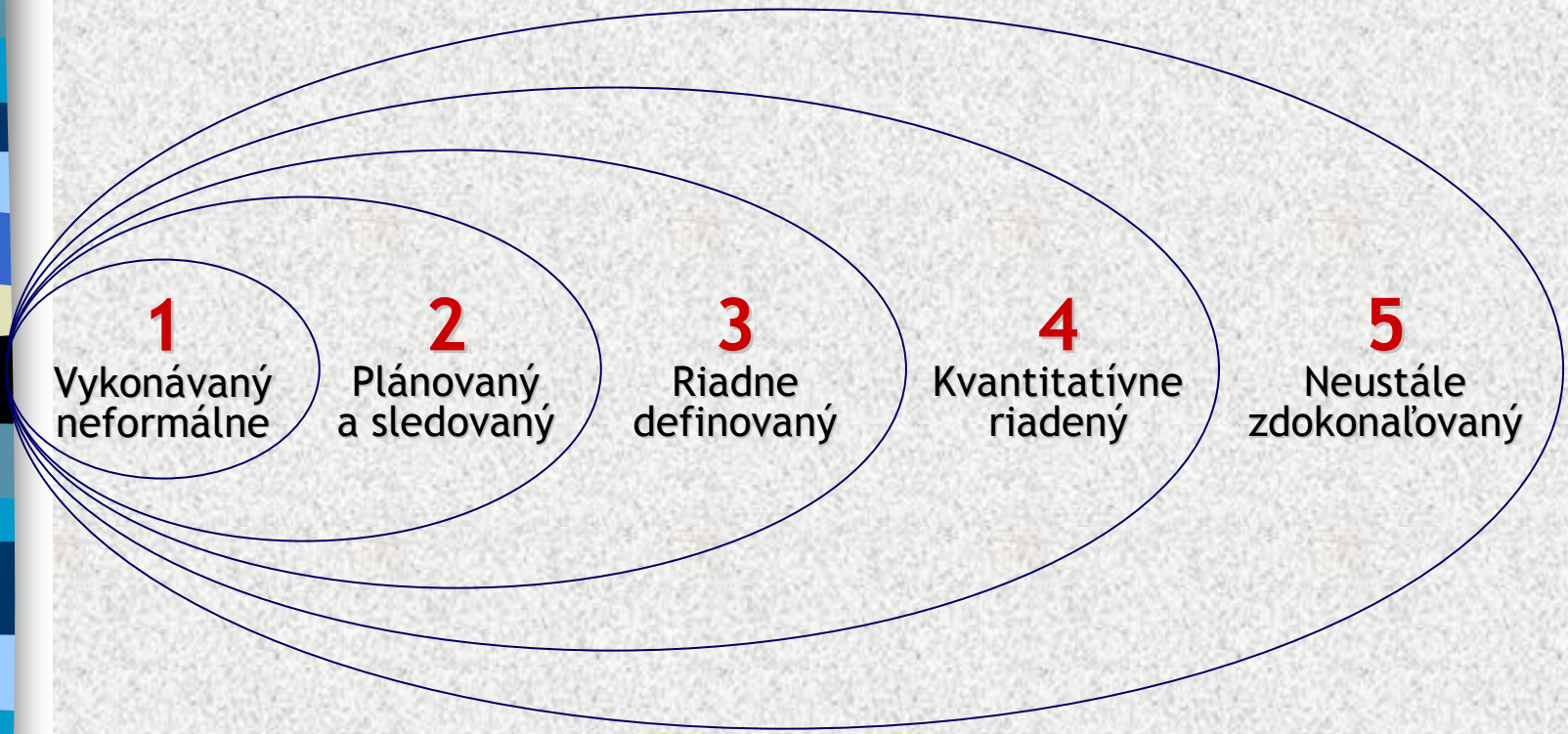


Ladislav Hudec

Životný cyklus programu bezpečnosti

Ladislav Hudec

Úrovne vyspelosti bezpečnostného programu



Úroveň 3 dosahujú inštitúcie s dobrým bezpečnostným programom

Zákonné požiadavky na IB

- Zákon NR SR č. 241/2001 Z. z., O ochrane utajovaných skutočností a vykonávacie Vyhlášky
- Zákon NR SR č. 428/2002 Z.z. O ochrane osobných údajov
- Zákon NR SR č. 273/1994 Z. z. O zdravotných poisťovniach
- Zákon NR SR č. 211/2000 Z. z. O slobodnom prístupe k informáciám
- Zákon NR SR č. 215/2002 Z. z. O elektronickom podpise a vykonávacie Vyhlášky č. 537 až 542/2002
- Zákon NR SR č. 483/2001 Z. z. O bankách
- Obchodný zákon, Daňový zákon v platnom znení

Štandardy pre IB

- STN ISO/IEC TR 13335 – Návod pre manažment bezpečnosti IT
- STN ISO/IEC 17799 – Manažment informačnej bezpečnosti
- ISO/IEC 15408 – Kritériá hodnotenia bezpečnosti IT
- ISO 21827 - SSE – CMM (System Security Engineering – Capability Maturity Model)

ĎAKUJEM
ZA POZORNOSŤ

Ladislav Hudec