Policejní akademie ČR v Praze
Fakulta bezpečnostního managementru

Odhalování a vyšetřování kybernetické kriminality

Doc. RNDr. Josef Požár, CSc.

21. 6. 2011

Osnova

1. Odhalování kybernetické kriminality
   - Typické situace
2 Trestně právní aspekty kybernetické kriminality
3. Vyšetřování kybernetické kriminality
   - Způsoby vyšetřování kybernetické kriminality
   - Vyšetřovací situace

Osnova

3. Organizace boje proti kybernetické kriminalitě
4. Závěr

1. Odhalování kybernetické kriminality

- **Kriminální situace kybernetické kriminality:**
  - **zjištění totožnosti pachatele,**
  - **způsob spáchání tr. činu – Modus Operandi.**
- **Evidentní a latentní trestná činnost**
  - **Operativně pátrací činnost policie - agenti, technika apod.**
  - **Oznámení kontrolních orgánů.**
  - **Ústní, telefonické, písemné oznámení.**
  - **Anonymy, soukromé bezpečnostní služby.**

Typické situace

Totožnost pachatele	ZSUTČ - Modus operandi
0	0
0	1
1	0
1	1

2. Trestně právní aspekty

- Útok proti počítači
  - § 205 tr.z.- krádež,
  - § 209 tr.z.- podvod
  - § 228 tr.z.- poškozování cizí věci.
- Útok proti programovému vybavení a datům
  - § 230 tr.z. – zneužití záznamu nosiče dat.
- Elektronické výpalné
  - §235 tr. z.– vydírání.

2. Trestně právní aspekty

- Útoky na osobní data – zák. č. 101/2000 Sb.
- Zneužívání výpočetní techniky pro osobní účely
  - § 207 tr.z.- neoprávněné užívání cizí věci.
- Porušování autorských práv - § 152 tr. z.
- Neoprávněné nakládání s osobními údaji - § 178 tr. z.

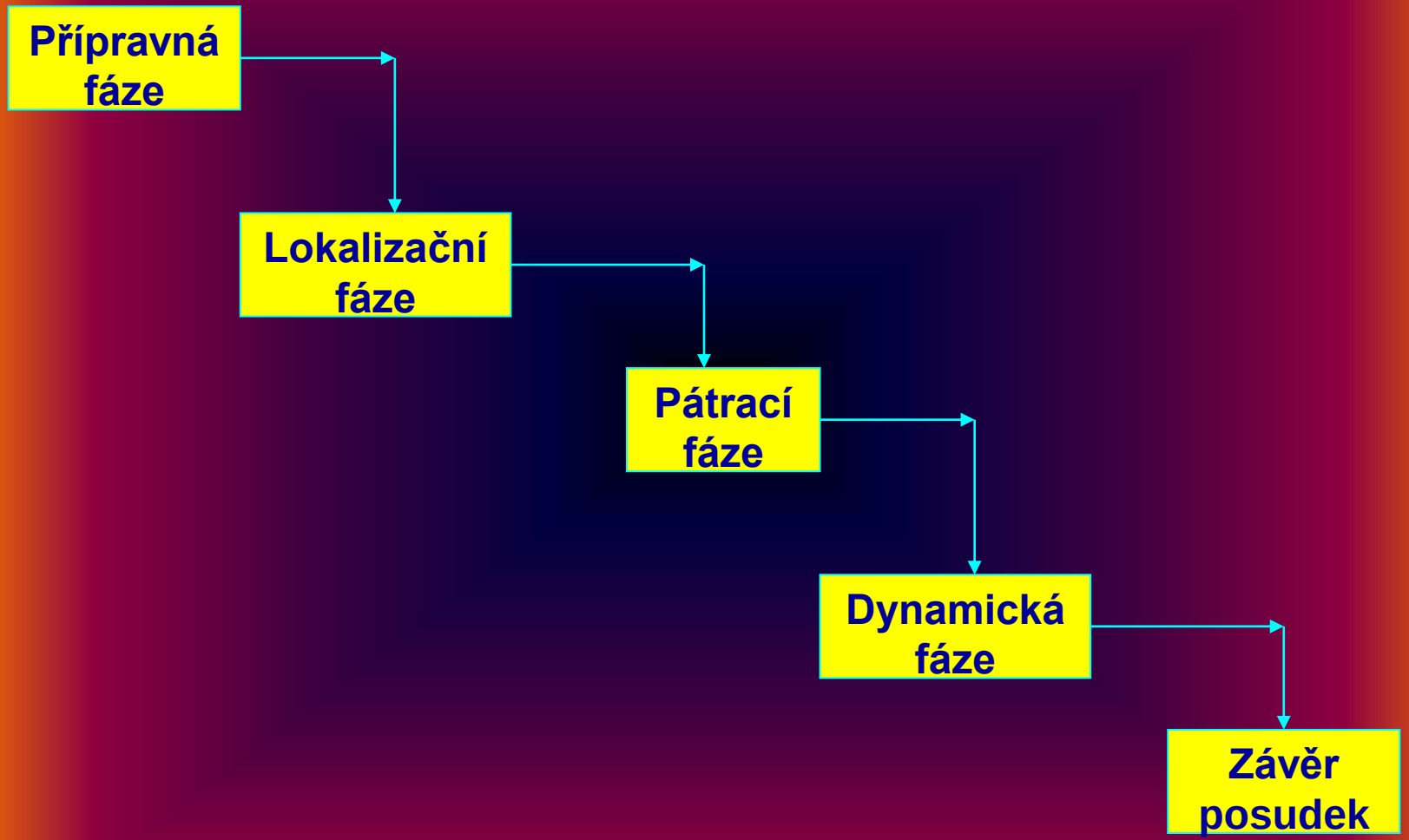
2. Trestně právní aspekty

- § 316 tr.z. – vyzvědačství,
- § 317 tr.z - ohrožení utajované informace, § 318 – z nedbalosti,
- Softwarové pirátství - porušování autorského zákona č. 121/2000 Sb.

3. Vyšetřování kybernetické kriminality

Oblasti vyšetřování kybernetické kriminality

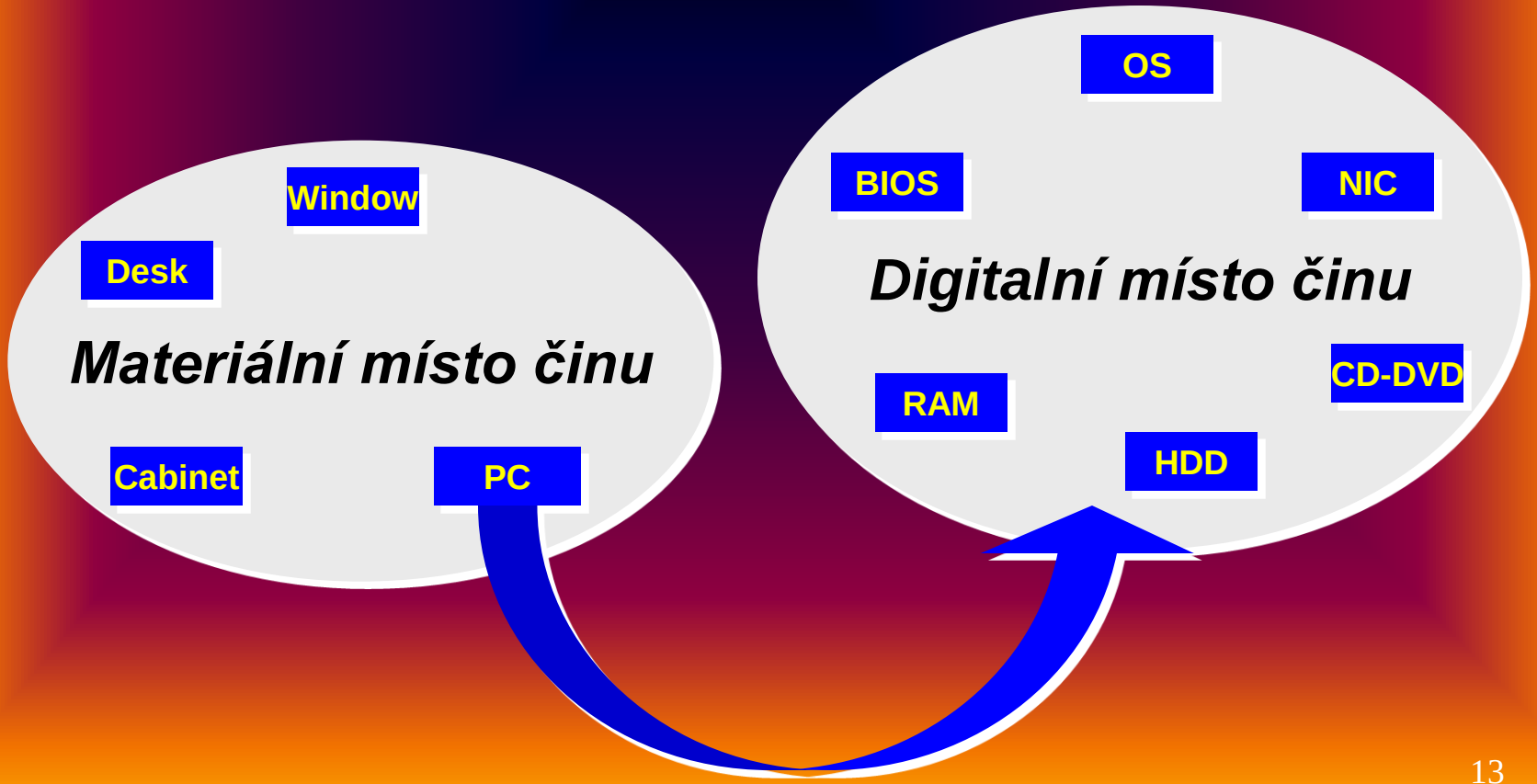
Obecný postup vyšetřování KK



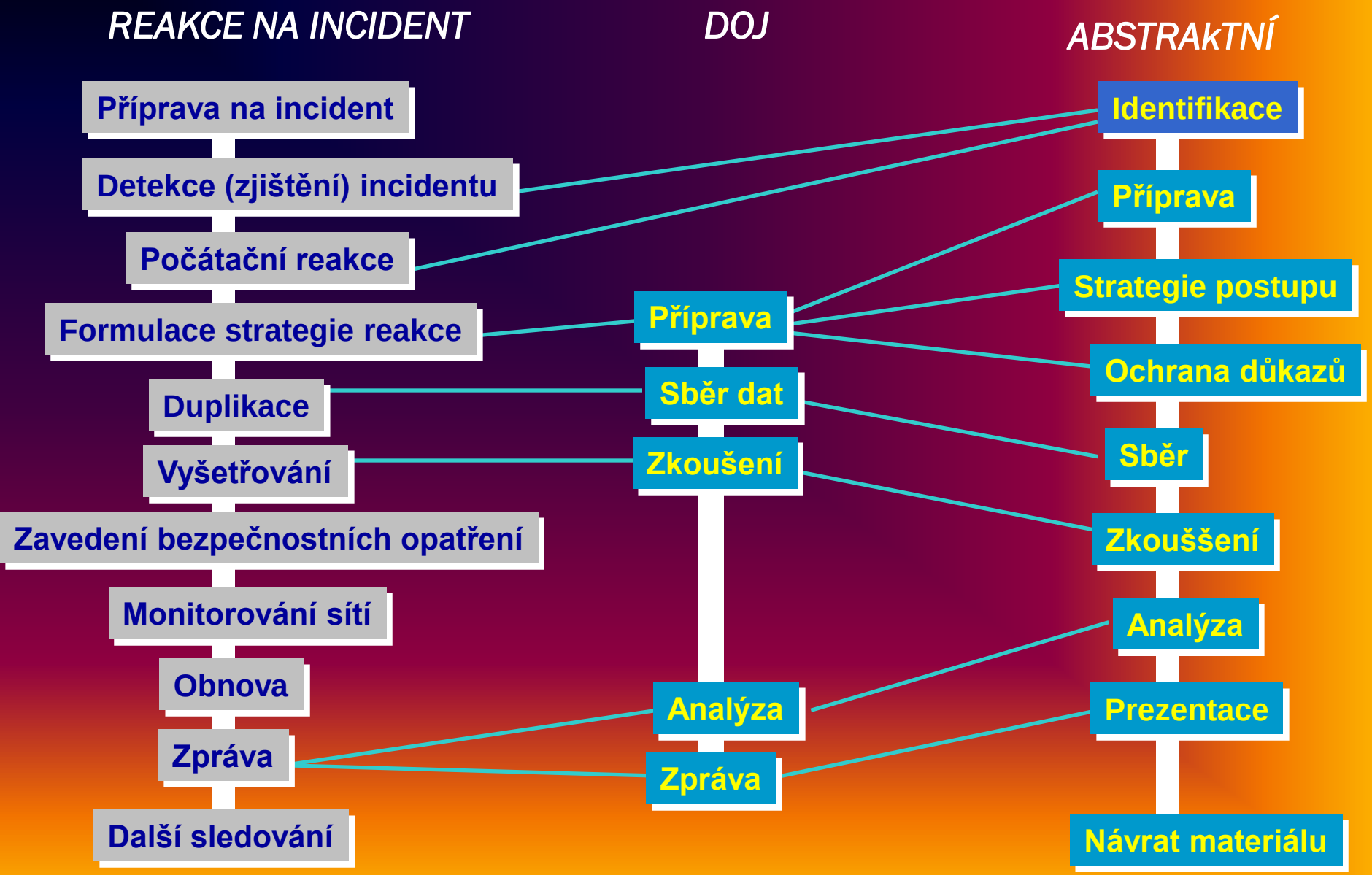
Postup vyšetřování kybernetické kriminality

- Materiální a digitální stopy.
- Ohledání místa trestného činu.
- Subjektivní a objektivní stránka trestného činu.
- Počáteční úkony a opatření na místě trestného činu.
- Zajišťovací úkony pro forenzní zkoumání.

Materiální a digitální místo činu



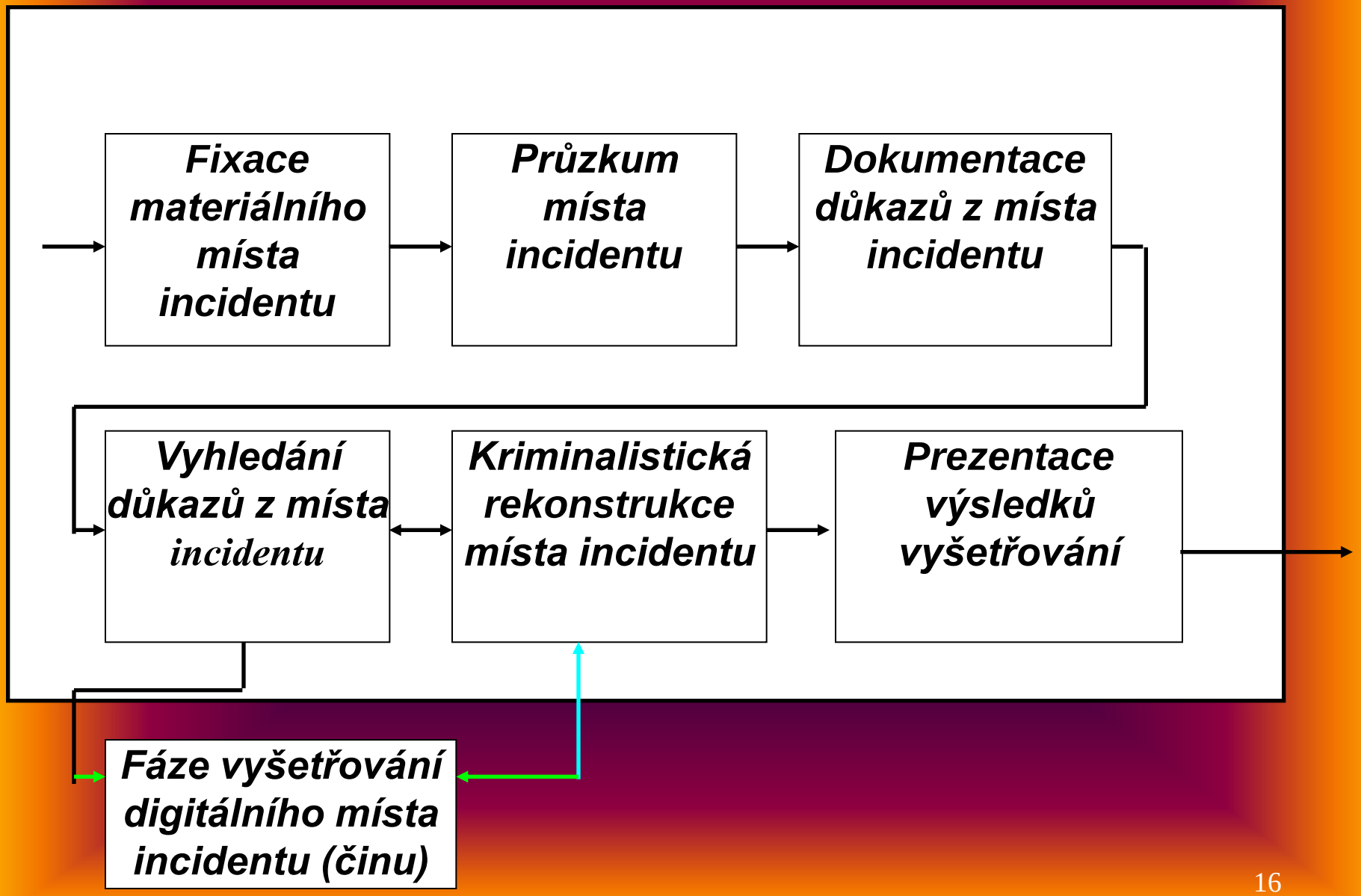
Komparace přístupů vyšetřování KK



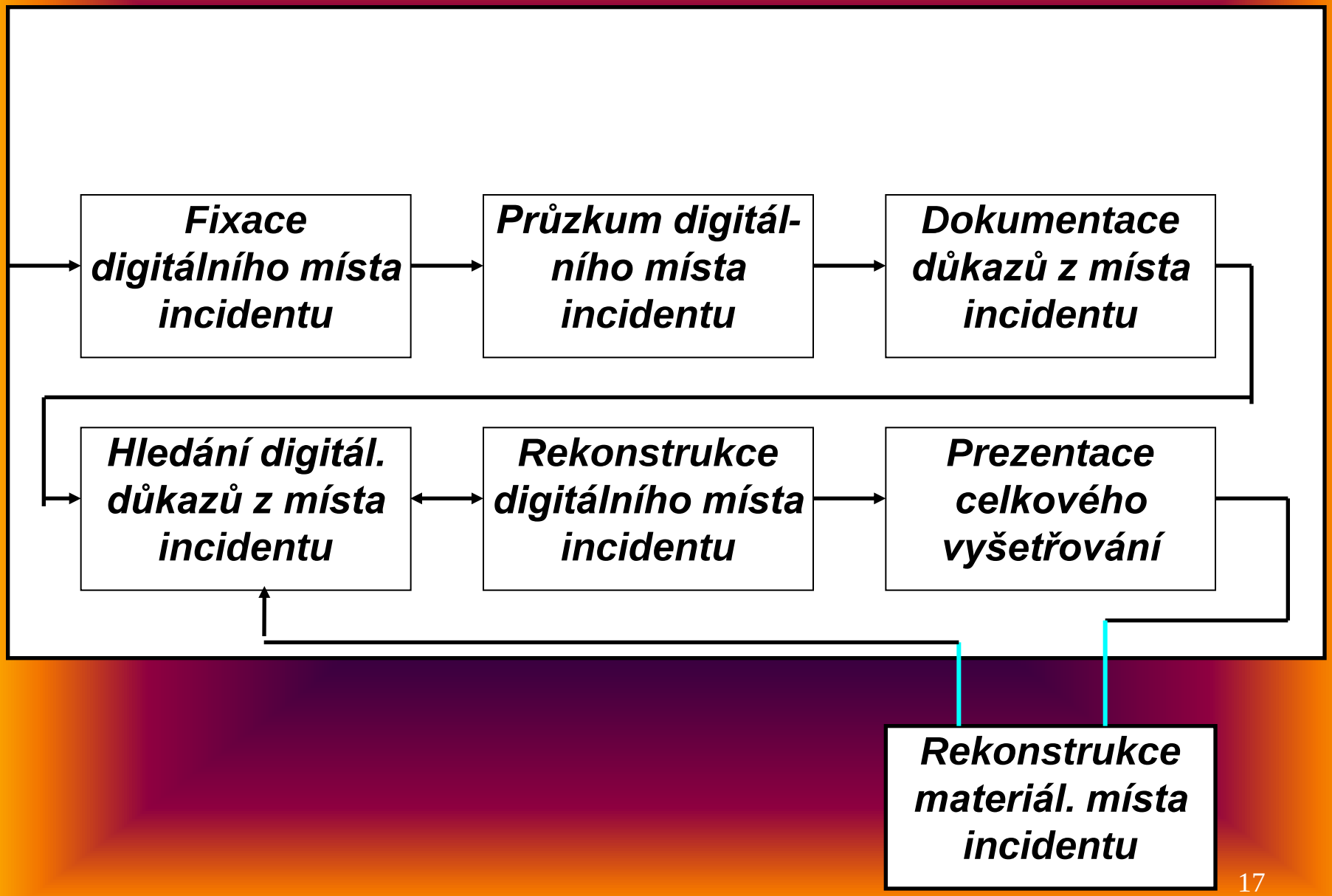
Integrovaný přístup k vyšetřování

- Přípravné stadium
  - Fáze operační přípravy
  - Fáze přípravy infrastruktury
- Dislokační stadium
  - Detekce a oznamovací fáze
  - Fáze potvrzení a autorizace
- Stadium materiálního vyšetřování
- Stadium digitálního vyšetřování
- Závěrečné hodnocení

Fáze materiálního stadia vyšetřování



Fáze digitálního stadia vyšetřování



Zpracování důkazů analýzy kybernetické kriminality

Identifikace → Sběr, pozorování a uchování → Analýza a organizace → Ověření

4 hlavní úkoly při zpracování digitálních důkazů

Identifikace: Každá digitální informace nebo její část, která může být použita jako důkaz.

Sběr, pozorování a uložení důkazů.

Analýza, identifikace a organizace důkazů.

Obnovení důkazů nebo opakování situace při verifikaci stejných výsledků ve stejném čase. Kontrola hashovací hodnoty.


NÁSTĚNKA
MONITOR
POZNÁMKY
Disky
MANUÁLY
POZNÁMKY
ODPADKY
DIÁŘE
KABELY-SPOJENÍ

3. Organizace boje proti KK

- Oddělení informační kriminality úřadu kriminální služby a vyšetřování P ČR.
- Zvýšení mezinárodní spolupráce na úseku informační bezpečnosti.
- Revize právních systémů a tvorbou mezinárodně uznávaných standardů.
- Vyvinout urychlené postupy pro získání provozních dat.

4. Závěry

- Rychlejší rozvoj informačních a komunikačních technologií – ještě rychlejší růst kybernetických prostředků i hrozeb a útoků na ně.
- Úroveň zákona: je třeba mít dobré zákony.
- Úroveň konvence: jde o ustálené kódy chování.
- Úroveň morální: to, co nám bylo vštípeno výchovou a kulturou již v dětství.