

# Učebné texty Postgraduálneho štúdia informačnej bezpečnosti

---

Toto CD obsahuje písomné materiály postgraduálneho kurzu Informačnej bezpečnosti, organizovaného MF SR v období september – december 2014. Materiály sú rozdelené na dve časti:

- texty prednášok, ktoré odzneli na postgraduálnom kurze a
- učebnica informačnej bezpečnosti.

Podľa Zmluvy o poskytovaní služieb pri vypracovaní štandardov základných znalostí, metodických materiálov, analýz dokumentov a súvisiacich vykonávacích predpisov a realizácii školení pre oblasť informačnej bezpečnosti uzavretej medzi MF SR a KPMG Slovensko, s.r.o. sú výstupom projektu len učebné texty. Keďže po pilotnom projekte boli zo strany MF SR vznesené na postgraduálne štúdium dodatočné obsahové požiadavky, ktoré zmluvne dohodnutý obsah učebnice nepokrýval, vytvorili sme Zborník prednášok, obsahujúci časť prednášok postgraduálu. (Témy, ktoré sú pokryté textami v učebnici, sme do Zborníka prednášok nezaradili.)

Obsah CD ROM je usporiadaný nasledovne:

1. UvodKCD (tento dokument)
2. OrganizaciaPGS (súbor obsahujúci plánovaný harmonogram PGŠ, zoznam autorov a názvy všetkých prednášok)
3. ZborníkPrednasok je adresár s tromi podadresármi, v ktorých sú umiestnené samotné prednášky v PDF formáte

## **Kryptológia**

1. Grošek O. Úvod do kryptoanalýzy klasických šifrier
2. Zajac P. Lineárna a diferenciálna kryptoanalýza
3. Zajac P. Postkvantová kryptografia
4. Repka M. Útoky cez postranné kanály proti ECC a McEliece algoritmom

## **Manažment informačnej bezpečnosti**

1. Jurčík M. Úvod do bezpečnostných incidentov
2. Hlavička L. Úvod do forenznej analýzy
3. Vargová Z. Hardening pracovnej stanice so systémom Windows 7

## **Bezpečnosť operačných systémov a sietí**

1. Ostertág R. Linux vo svete Windows

4. UcebницаPGS je adresár obsahujúci 4 súbory
  - 4.1. súbor **VK\_main**, obsahujúci dokument Vybrané kapitoly z informačnej bezpečnosti, (časť Manažment informačnej bezpečnosti a Elektronický podpis a PKI) (TeX, PDF)
  - 4.2. súbor **kryptologia** (TeX, PDF)
  - 4.3. súbor **BezpPocSieti** (pdf)

4.4. súbor **PokrocileBezpMechOSLinux-kniha** (pdf)

Do textov boli zapracované pripomienky odborného garanta a požiadavky MF SR.