

Základy kybernetické bezpečnosti

- [Základní studijní materiály](#)
- [Obsah kurzu](#)
- [Rozšiřující literatura](#)

Základní studijní materiály

Jan Kolouch, Pavel Bašta a kol.: CyberSecurity

Martin Hromada, Petr Hrůza a kol.: Kybernetická bezpečnost teorie a praxe

Jan Kolouch: CyberCrime

Petr Hrůza: Kybernetická bezpečnost

Petr Hrůza a kol.: Kybernetická bezpečnost II

Petr Jirásek, Ludek Novák a Josef Požár: Výkladový slovník Kybernetické bezpečnosti

Obsah kurzu

- 1. Typy kybernetických útoků**
- 2. Principy bezpečnosti IS/ICT.**
- 3. Metody zabezpečení podnikových IS/ICT.**
- 4. Sociální inženýrství.**
- 5. Monitoring ICT infrastruktury/ICT systémů.**
- 6. Základy moderní kryptografie.**
- 7. Práce s normami a jejich využití v podnikové praxi.**
- 8. Metodiky hodnocení informačního systému a infrastruktury.**
9. Detekce a obrana proti phishingu, praktické ukázky sociálního inženýrství.
10. Druhy virů – Spyware, malware, trojský kůň a jiné.
11. Sledování systému a sítě, detekce anomálií.
12. Forenzní postupy.
13. Šifrování.
14. Elektronický podpis.
15. Certifikáty.

Rozšiřující literatura

<u>Cyber Security</u>