1. Úvod do kybernetické bezpečnosti - základní pojetí (2p), Hrůza p
2. Normy a zákony kybernetické bezpečnosti. Ochrana utajovaných informací a určení neutajovaných informací (4p), Hrůza p
3. Systém řízení bezpečnosti informací (ISMS) (4p+2c), Hrůza p, c
4. Management kybernetické bezpečnosti a bezpečnostní role (2p+2c), Hrůza p, c
5. Soubor postupů pro management kybernetické bezpečnosti (4p+2c), Hrůza p, c
6. Hrozby a rizika v kyberprostoru. Ochrana aktiv. (2p+2s), Hrůza p, s
7. Audit a certifikace systémů řízení bezpečnosti informací (2p+2c), Hrůza p, c
8. Kritická informační infrastruktura a významné informační systémy (2p), Hrůza p
9. Hacker, typologie hackerů, hackerské skupiny (2p+2c), Hrůza p, c
10. Sociální inženýrství v kyberprostoru. Digitální stopa (2p+2c), Hrůza p, c
11. Koncepce kybernetické bezpečnosti a obrany v ČR a EU (2p+2s), Hrůza p, s
12. Úloha a poslání KYPO/MU (2exkurze), Hrůza e
13. Úloha a poslání NÚKIB (4exkurze), Hrůza e
14. Závěrečný seminář s obhajobou případové studie (6s) Hrůza s