VZDĚLÁVÁNÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI NA UNIVERZITĚ OBRANY
I. ČÁST

pplk. Ing. Petr HRŮZA, Ph.D.
petr.hruza@unob.cz
Univerzita obrany
Brno

Struktura Univerzity obrany

- Fakulta vojenského leadershipu (dříve FEM - Brno)
- Fakulta vojenských technologií (Brno)
- Fakulta vojenského zdravotnictví (Hradec Králové)

- Centrum bezpečnostních a vojenskostrategických studií
- Centrum jazykového vzdělávání (Brno)
- Centrum tělesné výchovy a sportu (Brno)
- Ústav ochrany proti zbraním hromadného ničení (Vyškov)

Fakulta vojenského leadershipu (FVL)

FVL má akreditovaný bakalářský studijní program „**Ekonomika a management**“. Program se dále dělí na studijní obory a studijní moduly. V oboru „**Bezpečnostní management**“ existuje modul „**Kybernetická bezpečnost**“.

Studijní modul je zaměřen na přípravu odborníků pro výkon analytických a manažerských funkcí v organizačních strukturách subjektů obrany a bezpečnosti České republiky v oblasti řízení procesů souvisejících se zajišťováním bezpečnosti informačních systémů.

Akreditováno pro vojenské i civilní studium, forma výuky prezenční i kombinovaná (civilní prezenční studium).

Studijní modul Kybernetická bezpečnost

Obsahuje předměty:

Teoretického základu (Management, KIT a NEC, Informatika, Právo, Základy operačního výzkumu, …).

Oborové (Společenské aspekty bezpečnosti, Metodologie analýzy rizik, Řízení bezpečnosti osob a společnosti, Aplikovaná informatika, Logistika v oblasti bezpečnosti).

Modulové (Management kybernetické bezpečnosti, Krizový management kybernetické bezpečnosti, Kybernetická a informační válka, Problémy mezinárodní bezpečnosti, *Bezpečnostní technologie, Komunikační a informační systémy a jejich bezpečnost*, Kybernetická kriminalita, Právní rámec kybernetické bezpečnosti).

Management kybernetické bezpečnosti

1. semestr

1. Základní východiska a normy informačního managementu
2. Systém řízení bezpečnosti informací
3. Soubor postupů pro management bezpečnosti informací

2. semestr

1. Základy procesního řízení
2. Základy projektového řízení
3. Řízení rizik bezpečnosti informací
4. Řízení aktiv kybernetické bezpečnosti
5. Metriky a měření pro hodnocení účinnosti zavedeného ISMS

Management kybernetické bezpečnosti

3. semestr

1. Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací
2. Zpracování případové studie a její obhajoba
3. Datové sklady a dataminig
4. Kryptografické techniky – Moderní kryptografické služby
5. Koncepce kybernetické obrany v EU a ostatních zemích
6. Kybernetická bezpečnost a kritická infrastruktura

Krizový management KB

1. semestr

1. Ochrana obyvatelstva - Normy ochrany obyvatelstva v EU a ČR
2. Havarijní plánování
3. Úloha expertů při řešení krizových situací
4. Katastrofy a hromadná neštěstí
5. Řešení krizových situací

Krizový management KB

2. semestr

1. Rozvoj klíčových kompetencí manažera
2. Potřeby a reakce lidí zasažených mimořádnou událostí
3. Metody prevence a efektivního zvládání zátěže a stresu
4. Kompetence manažera pro zvládání komunikace v zátěžových situacích
5. Komunikace manažera s lidmi zasaženými mimořádnou událostí
6. Praktické postupy v krizové komunikaci
7. Individuální a sociokulturní faktory ovlivňující porozumění významu sdělovaného
8. Základní komunikační techniky a jejich využití v krizovém řízení
9. Připravená a nepřipravená komunikace

Kybernetická a informační válka

1. Kyberprostor
2. Hrozby a rizika v kyberprostoru
3. Kyberprostor a islámský terorismus
4. Způsoby a nástroje hackingu
5. Média v informační společnosti, ozbrojených konfliktech a válečné zpravodajství
6. Kybernetické války a metody informačního boje, informační válka, typy informační války
7. Psychologické operace a vojenské klamání v armádách NATO
8. Útoky na informační systémy (taxonomie útoků, identifikace zdrojů)
9. Ochrana a obrana proti kybernetickým útokům