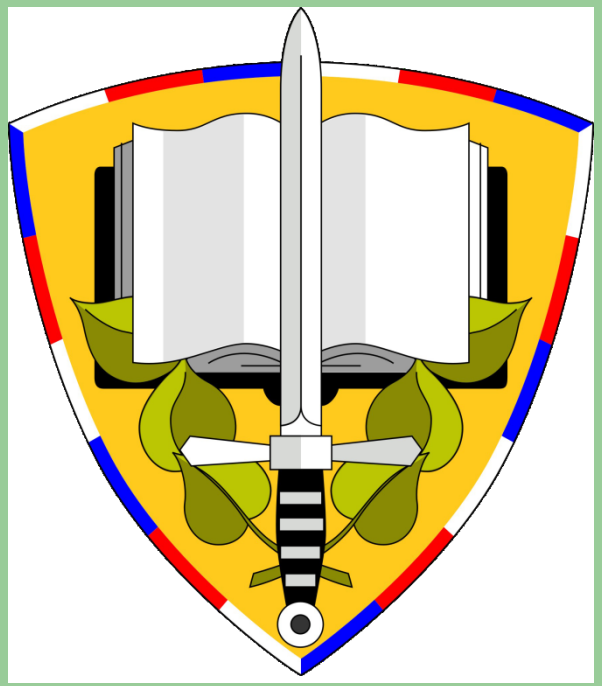
Kybernetická bezpečnost
-
nový trend ve vzdělávání



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

Kybernetická bezpečnost

Kybernetická bezpečnost je celosvětově vysoce aktuální a je jednou z klíčových výzev současnosti na celém světě. Kybernetické incidenty patří dnes mezi nejzávažnější hrozby pro společnost ve všech vyspělých zemích světa.

Univerzita obrany připravuje vojenské profesionály a další odborníky působící ve sféře bezpečnosti a obrany státu.

Struktura bakalářského studijního programu EKONOMIKA A MANAGEMENT

Ekonomika a management:

- Ekonomika obrany státu:
  - …
- Vojenský management:
  - …
- **Bezpečnostní management:**
  - **Kybernetická bezpečnost**
  - …

Charakteristika studijního oboru

BEZPEČNOSTNÍ MANAGEMENT

- Studium v oboru je vedle obecné oblasti ekonomiky a managementu zaměřeno na management ve specifických podmínkách organizací zapojených do zajišťování bezpečnosti, a to jak ve veřejném, tak i soukromém sektoru.

- Studenti si osvojují základní znalosti a dovednosti z oblasti:
  - krizového managementu,
  - řízení rizik,
  - řízení zdrojů v oblasti bezpečnosti,
  - bezpečnosti informačních systémů,
  - využívání informačních systémů pro zajišťování bezpečnosti a souvisejících společenských aspektů.

Charakteristika studijního modulu
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.
- Bakalářský studijní program.
- Vojenské i civilní studium.
- Forma výuky prezenční i kombinovaná.

Charakteristika studijního modulu
KYBERNETICKÁ BEZPEČNOST

Předměty:

- **Teoretického základu** (Management, KIT a NEC, Informatika, Právo, Základy operačního výzkumu, Dějiny, …).
- **Oborových** (Společenské aspekty bezpečnosti, Metodologie analýzy rizik, Řízení bezpečnosti osob a společnosti, Aplikovaná informatika, Logistika v oblasti bezpečnosti)
- **Modulových.**

Charakteristika studijního modulu
KYBERNETICKÁ BEZPEČNOST

Modulové předměty:

- Problémy mezinárodní bezpečnosti,
- Kybernetická a informační válka,
- Management kybernetické bezpečnosti,
- Bezpečnostní technologie,
- Komunikační a informační systémy a jejich bezpečnost,
- Krizový management kybernetické bezpečnosti,
- Kybernetická kriminalita,
- Právní rámec kybernetické bezpečnosti,
- Sociální prostředí a sociálně nežádoucí jevy.

PROBLÉMY MEZINÁRODNÍ BEZPEČNOSTI

Cíl předmětu:

Student se seznámí s historií řešení základních otázek mezinárodní bezpečnosti a s historickými souvislostmi vzniku, současnými projevy a možnostmi eliminace soudobých hrozeb. Student bude umět využít získané poznatky při analýze bezpečnostních rizik v současnosti. Student bude schopen vnímat závažnost celého spektra vojenských i nevojenských hrozeb, prezentovat základní poznatky o možnostech řešení projevů, extremismu a terorismu v současnosti.

PROBLÉMY MEZINÁRODNÍ BEZPEČNOSTI

Obsah a osnova předmětu:

1. Řešení základních problémů a konfliktů v mezinárodní bezpečnosti.
2. Ekonomická dimenze mezinárodní bezpečnosti.
3. Ekologická dimenze mezinárodní bezpečnosti.
4. Societální dimenze mezinárodní bezpečnosti.
5. Souvislosti vzniku a projevy politického a náboženského extremismu a terorismu v současnosti.
6. Úloha mezinárodních institucí a organizací (NATO, OSN, EU) při řešení bezpečnostních problémů.

KYBERNETICKÁ A INFORMAČNÍ VÁLKA

Cíl předmětu:

Studenti předmětu budou seznámeni se současnými koncepcemi, kategoriemi a metodami informační a kybernetické války, mezi něž patří kybernetické útoky na informační systémy a ochrana proti nim, psychologické operace, vojenské klamání, vztahy s veřejností a působení médií v ozbrojených konfliktech. Absolventi budou schopni řešit krizové situace a vzniklé následky informační a kybernetické války.

KYBERNETICKÁ A INFORMAČNÍ VÁLKA

Obsah a osnova předmětu:

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

MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

Cíl předmětu:

Hlavním cílem předmětu je, aby studenti získali ucelené poznatky z problematiky managementu kybernetické bezpečnosti. Seznámí se s vývojem a pojetím kybernetické bezpečnosti. Budou znát obsah, zásady, metody a nástroje kybernetického managementu, informační strategii, politiku a audit. Dále jim budou objasněny specifika činností informačního managementu v bezpečnostních složkách. Absolventi budou znát role a působnost informačního manažera se zaměřením na kybernetickou bezpečnost.

MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

Obsah a osnova předmětu:

1. Vymezení kybernetické bezpečnosti a její rozměry
2. Pojetí managementu kybernetické bezpečnosti - cíle, nástroje a postupy
3. Politika, strategie a taktika kybernetické bezpečnosti
4. Soubor postupů pro management bezpečnosti informací
5. Hrozby, rizika a hodnocení kybernetické bezpečnosti
6. Kybernetická bezpečnost a kritická infrastruktura
7. Dokumenty a audit kybernetické bezpečnosti
8. Informační management a jeho obsah, role a působnost
9. Řízení rizik bezpečnosti informací
10. Koncepce kybernetické obrany v EU a NATO

BEZPEČNOSTNÍ TECHNOLOGIE

Cíl předmětu:

Předat základní teoretické poznatky o bezpečnostních technologiích komunikačních a informačních systémů a směry jejich vývoje. Seznámit s metodami implementace bezpečnostních prvků sítě, technologií AAA, firewallů, systémů detekce průniku, zabezpečení přepínačů, směrovačů, WiFi sítí a komponent IP telefonie a kryptografických systémů. Popsat manažerské postupy při zajištění sběru logů a auditních dat KIS, administraci (správě) systému, přidělování privilegií a rolí. Seznámit s bezpečnostními aspekty postupů jako je Business Continuity Planning, Disaster Recovery a System Development Life Cycle.

BEZPEČNOSTNÍ TECHNOLOGIE

Obsah a osnova předmětu:

1. Bezpečnostní hrozby ve vojenských sítích
2. Bezpečnostní prvky sítě
3. Autentizace, autorizace a evidence
4. Implementace techniky firewallu
5. Implementace systémů detekce průniku
6. Bezpečnost sítě LAN
7. Kryptografické systémy
8. Implementace sítí VPN
9. Bezpečnost bezdrátových sítí LAN
10. Bezpečnost IP telefonie
11. Management bezpečné sítě

KOMUNIKAČNÍ A INFORMAČNÍ SYSTÉMY A JEJICH BEZPEČNOST

Cíl předmětu:

Studenti předmětu budou znát podstatu komunikačního prostředí a zásady provozu na spojovacích prostředcích, bezpečnostní architekturu KIS. Dále budou seznámeni s IS používanými v AČR, se zranitelnostmi KIS a metodikou jejich testování, typickými bezpečnostními hrozbami a bezpečnostními opatřeními. Získané odborné znalosti a dovednosti budou umět používat při výkonu manažerských rolí na úrovni nižšího managementu. Budou schopni použít získané znalosti a dovednosti při praktickém výkonu své funkce.

KOMUNIKAČNÍ A INFORMAČNÍ SYSTÉMY A JEJICH BEZPEČNOST

Obsah a osnova předmětu:

1. Základy organizace spojení a požadavky na spojení
2. Šíření rádiových vln. Jednotlivé druhy spojení
3. Zásady vedení provozu na spojovacích prostředcích, dodržování provozní kázně
4. Ochrana spojovacích prostředků před rušením
5. Komunikační prostředky na stupni četa a možnosti jejich využití
6. Informační systémy a jejich struktura
7. Komunikační systémy
8. OTS VŘ PozS AČR
9. Organizace KIS v operacích AČR a NATO
10. Zranitelnosti KIS, identifikace rizik
11. Bezpečnostní hrozby
12. Struktura komunikační infrastruktury

KRIZOVÝ MANAGEMENT

Cíl předmětu:

Student se seznámí se zásadami ochrany obyvatelstva v EU, ČR, havarijního plánování, expertní podporou manažerů při řešení mimořádných událostí. Student bude umět aplikovat zásady havarijního plánování v praxi, podílet se na zvládání mimořádných událostí.

KRIZOVÝ MANAGEMENT

Obsah a osnova předmětu:

1. Ochrana obyvatelstva
2. Havarijní plánování
3. Úloha expertů při řešení krizových situací
4. Katastrofy a hromadná neštěstí
5. Řešení krizových situací
6. Rozvoj klíčových kompetencí manažera
7. Potřeby a reakce lidí zasažených mimořádnou událostí (stres, zátěž, krize)
8. Metody prevence a efektivního zvládání zátěže a stresu
9. Kompetence manažera pro zvládání komunikace v zátěžových situacích
10. Komunikace manažera s lidmi zasaženými mimořádnou událostí
11. Praktické postupy v krizové komunikaci
12. Individuální a sociokulturní faktory ovlivňující porozumění významu sdělovaného.
13. Základní komunikační techniky a jejich využití v krizovém řízení
14. Připravená a nepřipravená komunikace

KYBERNETICKÁ KRIMINALITA

Cíl předmětu:

Cílem předmětu je seznámit studenty s organizačními a legislativními zásadami prevence proti kybernetické kriminalitě, se základy práva v oblasti kybernetické kriminality a se zákonnými i podzákonnými normami kybernetické bezpečnosti. Studenti se budou po absolvování předmětu orientovat v systému práva v dané oblasti a budou umět aplikovat a realizovat nástroje k zajištění kybernetické bezpečnosti.

KYBERNETICKÁ KRIMINALITA

Obsah a osnova předmětu:

1. Listina základních práv a svobod, ochrana základních práv a svobod v AČR a ČR
2. Ochrana osobnosti, ochrana osobních údajů, ochrana informací v podmínkách AČR
3. Rozbor prostředí, servery, sítě, prvky sítě, typologie sítí.
4. Operační systémy, bezpečnost sítí, bezpečnost počítačů
5. Webové aplikace, bezpečnost úložišť dat
6. Elektronický důkaz, technické zabezpečení informačního prostoru
7. Modelové případy kybernetické kriminality projednávaných v ČR
8. Právní odpovědnost vyplývající z možné kybernetické kriminality

PRÁVNÍ RÁMEC KYBERNETICKÉ BEZPEČNOSTI

Cíl předmětu:

Cílem předmětu je seznámit studenty s legislativním rámcem kybernetické bezpečnosti a s formami páchání trestné činnosti v oblasti kybernetické bezpečnosti a jejich projednání u soudu.

PRÁVNÍ RÁMEC KYBERNETICKÉ BEZPEČNOSTI

Obsah a osnova předmětu:

1. Základy právního rámce kybernetické bezpečnosti
2. Hodnocení prostředí jako aktéra kybernetické bezpečnosti
3. Chování uživatele a osoba administrátora v systému kybernetické bezpečnosti
4. Právní odpovědnost vyplývající z kybernetické bezpečnosti
5. Formy páchání trestné činnosti v oblasti kybernetické bezpečnosti a projednání u soudu

SOCIÁLNÍ PROSTŘEDÍ A SOCIÁLNĚ NEŽÁDOUCÍ JEVY

Cíl předmětu:

Seznámit studenty s vybranými problémy z okruhu sociální patologie v kontextu informační společnosti. Blíže charakterizovat závažné negativní jevy a sociální deviace vyskytující se v moderních společnostech, které provázejí rozvoj informační společnosti. Seznámit s možnostmi využití poznatků a nástrojů sociologie a aplikovaných sociologických disciplín při studiu sociálně nežádoucích jevů souvisejících s kyberprostorem.

SOCIÁLNÍ PROSTŘEDÍ A SOCIÁLNĚ NEŽÁDOUCÍ JEVY

Obsah a osnova předmětu:

1. Využití sociologických poznatků při studiu SNJ
2. Informační společnost
3. Moderní společnost v reflexi sociologických teorií
4. Změny sociálních struktur
5. Problémy deskripce a explanace sociálního pohybu a změn v moderních společnostech
6. Sociálně nežádoucí jevy a sociální deviace
7. Sociálně nežádoucí jevy ve společnosti, projevy, příčiny a možnosti prevence
8. Komputerizace společnosti a její sociální důsledky
9. Informační a komunikační technologie vzdělávání
10. Digitalizace životního stylu a jeho sociální důsledky
11. Sociologický výzkum a jeho využití při studiu SNJ
12. Základní nástroje výzkumu
13. Média a společnost
14. Média a publikum
15. Vliv médií - závislosti
16. Prevence SNJ

ZÁVĚR

Studijní modul Kybernetická bezpečnost jako součást studijního oboru Bezpečnostní management je nově akreditovaným studijním modulem na Univerzitě obrany.

Jedná se o ojedinělý modul v systému vzdělávání v České republice. Všechny obdobné moduly na jiných vysokých školách v České republice jsou více zaměřeny na technickou stránku řešení kybernetické bezpečnosti.

DĚKUJI ZA POZORNOST

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

(https://appl.unob.cz/SeznamAkrStudProgWeb/index.aspx)