UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

TÉMATICKÝ OKRUH VOLITELNÉHO PŘEDMĚTU

INFORMATIKA V OCHRANĚ OSOB

K ODBORNÉ ROZPRAVĚ KONANÉ V RÁMCI STÁTNÍ ZÁVĚREČNÉ ZKOUŠKY
BAKALÁŘSKÉHO STUDIJNÍHO PROGRAMU

OCHRANA OBYVATELSTVA

Předměty okruhu

Aplikovaná informatika
Výukové simulace v ochraně obyvatelstva
Informační bezpečnost

Uherské Hradiště, 2024

1. **Algoritmizace úloh**
   (Základní terminologie a principy tvorby algoritmů, možnosti zápisu algoritmů, základní značky a pravidla pro tvorbu vývojových diagramů, příklad vývojového diagramu).

2. **Model, modelování. Simulace. Návrh simulačního experimentu**
   (Základní pojmy a principy modelování, definice modelu, dělení modelů, postup tvorby modelu, význam modelování v ochraně obyvatelstva, SW nástroj pro modelování úniků nebezpečných látek Terex. Definice a vymezení základních pojmů v oblasti simulace, experiment simulace, typy simulace, význam simulace v ochraně obyvatelstva. Postup realizace simulačního experimentu, typy a způsoby simulačních experimentů, význam modelu v simulačním experimentu, model a postup jeho tvorby).

3. **Praktická aplikace modelování**
   (Význam modelování v ochraně obyvatelstva, definice modelu a LS, funkční princip základních typů limnigrafických stanic, příklad modelu měrného profilu a výpočet průtoku pro statický model, parametry modelu volí student).

4. **Informační podpora, informační systémy a SW aplikace v ochraně obyvatelstva**
   (Definice informační podpory, obecné nástroje informační podpory – informační systémy, nástroje a formy informační podpory v ochraně, příklady nástrojů informační podpory v ochraně obyvatelstva. Definice informačního systému (IS), základní komponenty a funkce IS, životní cyklus IS, příklady IS v oblasti ochrany obyvatelstva, význam SW aplikací v ochraně obyvatelstva, jejich úloha a přínos, popis a úloha jednotlivých systémů: Riskan, Terex, Terinos, ISKŘ, Argis, Kiskan, Krizkom).

5. **Geografické informační systémy**
   (Definice geografického informačního systému (GIS), prostorová data, geoobjekt a jeho typy, základní typy úloh řešitelných v GIS, postup práce v GIS, význam GIS v bezpečnostních aplikacích, příklady GIS).

6. **Geografické informační systémy – mapování rizik**
   (Základní principy mapování rizik v GIS, komparace mapování rizik s konzervativními metodami analýzy rizik, mapa hrozby a zranitelnosti, mapa rizika, kumulované riziko).

7. **Počítačové sítě**
   (Základní pojmy a definice, přenosová média, typy konstrukce a princip přenosu signálu, topologie počítačových sítí Význam počítačových sítí v ochraně obyvatelstva).

8. **Model, modelování**
   (Základní pojmy a principy modelování, definice modelu, dělení modelů, postup tvorby modelu, význam modelování v ochraně obyvatelstva, SW nástroj pro modelování úniků nebezpečných látek Terex).

9. **Živá simulace**
   (Definice živé simulace, základní principy, scénáře činností v ochraně obyvatelstva, základní dokumentace k realizaci cvičení v ochraně obyvatelstva).

10. **Virtuální simulace**
    (Definice, vymezení v kontextu pojmu simulace, základní principy, zajištění, význam v ochraně obyvatelstva).

11. **Konstruktivní simulace**
    (Definice, vymezení v kontextu pojmu simulace, základní principy, zajištění, význam v ochraně obyvatelstva).

12. **Výuková simulace, scénáře**
    (Definice, vymezení v kontextu pojmu simulace, základní principy, zajištění, význam v ochraně obyvatelstva. Definice a typy scénářů, postup tvorby scénářů, úloha a význam scénářů v simulaci, význam scénářů v ochraně obyvatelstva).

13. **Simulátory a technická podpora simulace**
    (Základní typy technického vybavení v podpoře simulace, moderní trendy v HW vybavení, příklady využití v simulaci v ochraně obyvatelstva).

14. **Virtuální a rozšířená realita**
    (Vymezení pojmů, definice, princip činnosti, význam VR a AR v ochraně obyvatelstva).

15. **Základy informační a kybernetické bezpečnosti**
    (Základní názvosloví – informace, kyberprostor, informační bezpečnost, kybernetická bezpečnost, kybernetická bezpečnostní událost, kybernetický bezpečnostní incident a další. Související normy a právní předpisy – jejich výčet, charakteristiky a určení. Významné subjekty, jejich název a účel).

16. **Základní principy kybernetické a informační bezpečnosti**
    (Triáda CIA – definice jednotlivých komponent a způsoby jejich zajištění. Autentizace a autorizace – popis, dělení, příklady. Kryptologie – význam, dělení a popis, problematika hashování.).

17. **Kybernetické útoky**
    (Sociální inženýrství, phishing a spear phishing, pharming, DoS, DDoS, SPAM a další – jejich popis, specifikace. Příklady a popis významných historicky realizovaných kybernetických útoků v ČR i zahraničí – Stuxnet apod.).

18. **Malware**
    (Význam slova, dělení a specifikace z hlediska způsobu šíření, dělení a specifikace z hlediska efektu. Antimalware, firewall, SIEM a další prostředky ochrany pracovních stanic. Příklady a popis významných v historii realizovaných útoků za pomoci malware – Ransomware v Benešovské nemocnici apod.).

19. **Řízení kontinuity činností organizace z hlediska informační a kybernetické bezpečnosti**
    (Informační technologie (IT) a operační technologie (OT) – jejich definice, příklady. Analýza rizik v kontextu informační a kybernetické bezpečnosti – aktiva, hrozby, zranitelnosti, metody vhodné pro provedení analýzy rizik. Preventivní opatření, plán obnovy po havárii (DRP) a reaktivní opatření).

20. **Hrozby v kyberprostoru**

(Netolismus, nomofobie, sexting, kyber grooming, kyber stalking, kyber šikana, hatespeech, pornografie - jejich definice. Dezinformace, misinformace, deepfakes, sociální bubliny - jejich definice, příklady. Darkweb a anonymita na internetu – definice pojmů dark web a deep web, anonymní režim webového prohlížeče, Tor, VPN).

Literatura:

1. ČESKO. Zákon č. 181/2014, o kybernetické bezpečnosti. In: *Sbírka zákonů*. 2014, částka 75, číslo 181.
2. CHLAPEK, Dušan; ŘEPA, Václav a STANOVSKÁ, Iva. *Analýza a návrh informačních systémů*. Praha: Oeconomica, 2011. ISBN 978-80-245-1782-7.
3. JENSEN, John R. a JENSEN, Ryan R. *Introductory geographic information systems*. Pearson series in geographic information science. Boston: Pearson, c2013. ISBN 978-0-13-614776-3.
4. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. Praha: CZ.NIC, z.s.p.o.. CZ.NIC, 2019. ISBN 978-80-88168-31-7. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf
5. KOLOUCH, Jan. *CyberCrime* [online]. Praha: CZ.NIC, z.s.p.o.. CZ.NIC, 2016. ISBN 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf
6. KOMINÁCKÁ, Jitka. *Prostorově orientované systémy pro podporu manažerského rozhodování*. C.H. Beck pro praxi. Praha: C.H. Beck, 2007. ISBN 978-80-7179-463-9.
7. LUKÁŠ, Luděk a kolektiv. *Bezpečnostní technologie, systémy a management V.* Zlín, 2015. ISBN 978-80-87500-67-5.
8. MURRAY, Neil G. *Witness Horizon 24 simulation modeling: rational process design*. Great Britain: Independently published, 2021. ISBN 979-8701142990.
9. NEMANJIC, Boris a SVETOZAR Navenka, ed. *Computer simulations: technology, industrial applications and effects on learning*. New York: Nova Science Publishers. Computer science, technology and applications, 2013. ISBN 978-1-6225-7580-0.
10. SVOBODA, Petr. *Návrh algoritmu implementace virtuálních simulátorů do výcviku v průmyslu komerční bezpečnosti*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2019. Dostupné také z: https://digilib.k.utb.cz/handle/10563/45886
11. TAUFER, Ivan. *Algoritmy a algoritmizace - vývojové diagramy*. Pardubice: Univerzita Pardubice, 2009. ISBN 978-8-0739-5182-5.
12. WALLACE, Patricia. *Introduction to information systems*. Second edition. Boston: Pearson, 2015. ISBN 978-1-2920-7110-7.