Státní závěrečné zkoušky	Akad. rok 2021/2022
Magisterský studijní program:	Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní technologie, Bezpečnostní management

Ochrana informačních systémů

Předmět povinně volitelný

1. Maxwellovy rovnice v komunikačních systémech - Ampérův průtokový zákon, zákon elektromagnetické indukce, princip uzavřenosti magnetických indukčních čar, Gaussova věta elektrického pole.
2. Elektromagnetické pole - homogenní a nehomogenní prostředí, izotropní a anizotropní prostředí, podmínky na rozhraní dvou různých prostředí.
3. Vlnová délka, frekvence, rychlost elektromagnetických vln, energie elektromagnetických vln, elektromagnetické spektrum (ionizující a neionizující záření), rádiové vlny a mikrovlny a jejich použití v technických systémech.
4. Míry intenzity elektromagnetického pole, blízké a vzdálené pole, jevy šíření - odraz, lom, interference, útlum, rozptyl, technické důsledky šíření elektromagnetických vln.
5. Umělé a přirozené zdroje elektromagnetického pole, princip mobilních telefonů, vývoj komunikačních systémů - technologie 5G, legislativní dokumenty.
6. Systém řízení informační bezpečnosti, analýza a řízení rizik informační bezpečnosti. Zákony, normy a předpisy související s bezpečností informačních systémů a kybernetickou bezpečností.
7. Hašovací funkce, vlastnosti funkcí MD a SHA, využití hašovacích funkcí v průmyslu a veřejné správě. Možnosti využití hašovacích algoritmů ve SMART technologiích.
8. Správa Identit a přístupů (IAM – Identity and Access Management). Řízení přístupů. Adresářové systémy. Provisioning. Architektura IAM řešení. Pokročilé technologie pro správu identit. Správa identit a přístupů v prostředí Internetu. Budoucnost digitálních identit.
9. Zabezpečení bezdrátových sítí - filtrování MAC adres, skrytí SSID, šifrování WEP, WPA a WPA2.
10. AAA koncept bezpečnosti (autentizace, autorizace, accounting), principy a aplikace, protokoly (TACACS, RADIUS) – principy, použití, jejich porovnání, výhody, nevýhody.
11. Technologie prevence průniku do IS, firewall, IDS, IPS, princip činnosti, začlenění do sítě, porovnání – výhody a nevýhody.
12. Koncept VPN, princip, účel, využití tunelování pro přenos ve VPN, technologie GRE, IPSec, SSL, protokoly, principy využití, porovnání- výhody, nevýhody, cloud computing.
13. 3D model informační bezpečnosti, hrozby, požadavky informační bezpečnosti, management rizik v oblasti informační bezpečnosti, bezpečnostní politika, kriteria hodnocení, metody a standardy.
14. Šifrování a kódování, vztah a rozdíl, základní pojmy: abeceda OT a ŠT, klíčový prostor a vztahy pro jeho výpočet, symetrická, asymetrická a hybridní kryptografie – principy, výhody a nevýhody, steganografie – principy, rozdělení a příklady.
15. Klasická kryptografie: substituční a transpoziční systémy – rozdíly mezi nimi a jejich kompletní rozdělení, příklady a principy vybraných nejvýznamnějších šifrovacích systémů.

16. Moderní kryptografie: symetrické proudové a blokové šifry – Vernamova šifra a další příklady moderních šifrovacích systémů, rozdíly, asymetrická kryptografie - jednosměrné kryptografické funkce, Diffie-Hellman Protokol, RSA.
17. Útoky na kryptografické systémy – rozdělení a popis nejzákladnějších útoků na šifrovací systémy, kryptoanalýza – popis a metody analýzy jednoduchých substitučních systémů, Vigenerovských substitučních systémů a moderních šifer.
18. Legitimní a nelegitimní důvody odposlechu komunikace na počítačové síti, princip odposlechu, popis jednotlivých částí snifferu a možností jeho umístění v síti, princip a zhodnocení možností obrany proti odposlechu v počítačové síti.
19. Forenzní analýzy dat. Přípravná fáze pro bezpečnou manipulaci se zajišťovanými daty. Analýzy dat na disku (uveďte nejčastější). Popište nejčastěji prováděné analýzy dat ze síťového provozu (nejčastěji hledané informace + konkrétní data, která lze v síťovém provozu najít). Jaké jsou omezující podmínky pro analýzu síťové komunikace.
20. Důvody realizace penetračních testů, charakteristika jednotlivých fází penetračního testu, dle jakých norem se testování provádí, nejčastěji testované objekty IT infrastruktury, srovnání penetračního testu s reálným útokem na infrastrukturu.