Státní závěrečné zkoušky	Akad. rok 2021/2022
Magisterský studijní program:	Inženýrská informatika
Obor:	Bezpečnostní technologie, systémy a management
Zaměření:	Technické, manažerské

Ochrana informačních systémů

Předmět povinně volitelný

1. Systémové požadavky na integrované poplachové systémy, charakteristika integrovaných poplachových systémů, použití, typy konfigurací, poplachové a nepoplachové aplikace.
2. Softwarová integrace poplachových a nepoplachových aplikací, funkce, obecné schéma, schéma základních vazeb klasifikace a popis softwarových produktů, klasifikace a práva uživatelů integračních SW, schéma základních systémových vazeb.
3. Systémová integrace - význam, principy systémové integrace, možnosti, formy systémové integrace, úloha systémového integrátora.
4. Integrované systémy nevýrobní automatizace – oblasti nevýrobní automatizace, význam a principy integrace, charakteristika systémového přístupu k integraci.
5. Systém řízení informační bezpečnosti, analýza a řízení rizik informační bezpečnosti. Zákony, normy a předpisy související s bezpečností informačních systémů a kybernetickou bezpečností.
6. Hašovací funkce, vlastnosti funkcí MD a SHA, využití hašovacích funkcí v průmyslu a veřejné správě. Možnosti využití hašovacích algoritmů ve SMART technologiích.
7. 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.
8. Zabezpečení bezdrátových sítí - filtrování MAC adres, skrytí SSID, šifrování WEP, WPA a WPA2.
9. AAA koncept bezpečnosti (autentizace, autorizace, accounting), principy a aplikace, protokoly (TACACS, RADIUS) – principy, použití, jejich porovnání, výhody, nevýhody.
10. Technologie prevence průniku do IS, firewall, IDS, IPS, princip činnosti, začlenění do sítě, porovnání – výhody a nevýhody.
11. Koncept VPN, princip, účel, využití tunelování pro přenos ve VPN, technologie GRE, IPSec, SSL, protokoly, principy využití, porovnání- výhody, nevýhody, cloud computing.
12. 3D model informační bezpečnosti, hrozby, požadavky informační bezpečnosti, management rizik v oblasti informační bezpečnosti, bezpečnostní politika, kriteria hodnocení, metody a standardy.
13. 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.
14. Klasická kryptografie: substituční a transpoziční systémy – rozdíly mezi nimi a jejich kompletní rozdělení, příklady a principy vybraných nejvýznamnějších šifrovacích systémů.
15. 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.

16. 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.
17. 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.
18. Metody maskování virového těla v hostitelském souboru, dekryptor viru, vymezení a způsob využití pro detekci virů, mutační engine DarkAvenger.
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.