<u>Předmět:</u> Bezpečnostní technologie a přístupy

<u>Otázky ke státní bakalářské zkoušce pro obor: Informační a síťová bezpečnost.</u>

Akademický rok 2025/2026

Vycházející z předmětů: Právo informačních technologií (KM/PRINF), Řízení projektů (KIT/ RPRO), Řízení bezpečnosti informací (KIT/RBI), Základy kryptografie a zabezpečení systémů (KIKM/ZKZBS), Řízení informačních rizik v praxi (KIT/RIRP), Bezpečnost webových technologií (KIT/ WEBS), Dohledové systémy a forenzní analýza (KIT/DSFA), Etický hacking (KIT/ETH), Bezpečnost databázových systémů (KIKM/SDBS), Bezpečnost počítačových sítí (KIT/BPSIT), Využití umělé inteligence v bezpečnosti (KIT/VUIB)

1) **Právo informačních technologií** (GDPR, právní rámec kybernetické bezpečnosti, právní delikty v oblasti IT, počítačová kriminalita, praktická aplikace práva v oblasti řízení kybernetické bezpečnosti, ochrany dat a compliance v IT prostředí).
2) **Principy projektového řízení** (základní pojmy, metodiky řízení projektů, principy sestavení harmonogramu a rozpočtu projektu, základní typy projektů a jejich náležitosti a rozsah, základní principy PRINCE2 (organizace projektu, Business Case, projektový tým, řízení rizik, plány, kvalita a změny, agilní metody řízení projektů) a SCRUM (role, události a artefakty).
3) **Řízení bezpečnosti informací** (architektura ISMS a jeho hlavní prvky, normy řady ISO/IEC 27000, role procesů jako je ITIL a COBIT v řízení bezpečnosti informací, model implementace a auditu ISMS).
4) **Symetrická kryptografie** (základy šifrování (pojmy šifrování, klíč, otevřený text, šifrový text), princip symetrického šifrování, rozdíl mezi blokovými a proudovými šiframi a příklady jejich využití, AES)
5) **Asymetrická kryptografie** (princip asymetrického šifrování, hybridní šifrování, digitální podpis a schéma podepisování, PKI a role certifikační autority, RSA, Diffie-Hellmanův protokol)
6) **Řízení informačních rizik** (životní cyklus kybernetické bezpečnosti, proces analýzy rizik podle normy ISO 27005, identifikace aktiv, hrozeb a zranitelností, kvantifikace rizik a postupy pro jejich mitigaci).
7) **Bezpečnost webových technologií** (nejčastější útoky na webové aplikace, klasifikace zranitelností; útoky na autentizaci, data a šifrovací algoritmy; skriptování na straně klienta, útoky na aplikační servery; bezpečnostní testování, metody a postupy testování; životní cyklus aplikace z pohledu bezpečnosti).
8) **Dohledové systémy** (základní principy a dělení dohledových systémů, role v systému ISMS, komunikační protokoly, architektura SIEM a Umbrella, principy korelačních pravidel a automatizace řešení pro zajištění bezpečnosti, modely implementace a analýza datových toků).
9) **Forenzní analýza IT/OT systémů** (úvod do forenzní analýzy, metodiky a postupy sběru stop, příprava a vyhodnocení analýzy, právní aspekty forenzní analýzy, metody pro analýzu IT a OT systémů).

10) **Etický hacking** (základní pojmy terminologie v oblasti ochrany informačních systémů a technologií, druhy hackingu, skeny zranitelností, penetrační testování, sandboxing a další technologie pro zajištění ochrany systémů, klíčové principy zranitelností a ochran operačních systémů na bázi Unixu a Widnows pro koncová, mobilní a serverová zařízení).
11) **Etický hacking** (kategorizace útočných technik a možnosti pro zajištění ochrany infrastruktury jako celku, kybernetické polygony, digitální dvojčata, simulační a testovací infrastruktury pro zvýšení bezpečnosti, sběr dat a vyhodnocování vektoru útoku (threat hunting), analýza a zajištění ochrany koncových stanic, řízení incidentů a reakce na útoky).
12) **Bezpečnost databázových systémů** (normalizace databáze, referenční integrita, transakce, zámky a kontrolní omezení, autentizace a autorizace, řízení přístupu k relačním databázím, zabezpečení ve fázích návrhu, implementace a produkce, zabezpečení NoSQL databází, anonymizace dat, auditování databází, best practice řešení pro komplexní zabezpečení).
13) **Bezpečnost počítačových sítí** (úvod do bezpečnosti počítačových sítí a aktuální trendy, zajištění bezpečnosti síťových zařízení, řízení, monitoring a automatizace síťových prvků, koncept autentizace, autorizace a účtování, firewallové technologie a architektura pro zvýšení bezpečnosti sítě, sondy a technologie pro detekci a prevenci průniků IDS/IPS).
14) **Bezpečnost počítačových sítí** (zabezpečení koncových zařízení, zajištění bezpečnosti LAN sítí, kryptografické systémy a jejich implementace v počítačových sítích, virtuální privátní sítě VPN a jejich implementace, nasazení moderního firewallu a zabezpečení sítě s důrazem na aplikační, webovou, DNS, IDS/IPS, kontrolu certifikátů a souvisejících nastavení).
15) **Umělá inteligence a strojové učení v kyberbezpečnosti** (klasické metody strojového učení – regrese, klasifikace), principy neuronových sítí, generativní AI, rizika zneužití AI a ML, bezpečnostní cíle při použití AI v detekci podvodných transakcí, malware a spamů).