Špecialista kybernetickej bezpečnosti

Rola:	**Špecialista kybernetickej bezpečnosti**	
Vedomosti:	**Riadenie bezpečnosti**	
	1) procesy, systémy a zásady riadenia informačnej a kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti	BL4
	2) zásady organizácie informačnej a kybernetickej bezpečnosti	BL4
	3) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti	BL5
	4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí	BL4
	5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (kľúčové ukazovatele výkonnosti – KPI, kľúčové ukazovatele rizík – KRI, metodiky merania vyspelosti atď.)	BL4
	6) zdroje, charakteristiky a použitie informačných aktív organizácie	BL5
	7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami	BL3
	8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI)	BL5
	9) procesy riadenia kontinuity činností a plánovania havarijnej obnovy prevádzky	BL5
	10) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.)	BL5
	11) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.)	BL5
	12) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly a sieťové služby	BL4
	13) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.)	BL5
	14) charakteristiky fyzických a virtuálnych nosičov údajov	BL5
	15) elektronické zariadenia (napr. počítačové systémy/komponenty, zariadenia na kontrolu prístupu, digitálne fotoaparáty, digitálne skenery, pevné disky, pamäťové karty, modemy, sieťové komponenty, sieťové zariadenia, sieťové domáce ovládacie zariadenia,	BL5

	tlačiarne, vymeniteľné úložné zariadenia, telefóny, faxy atď.)	
	16) elektrotechnika aplikovaná na architektúru počítačov (napr. základné dosky, procesory, čipy a iný počítačový hardvér)	BL2
	17) koncepcia a mechanizmy zálohovania a obnovy dát	BL4
	18) kryptografické algoritmy	BL4
	19) kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy)	BL4
	20) kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov (napr. symetrické šifry, asymetrické šifry, hašovacie funkcie, autentizačné kódy, digitálne podpisy)	BL4
	21) metódy a politiky správy a štandardizácie údajov	BL5
	22) nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti	BL6
	23) princípy dolovania a ukladania údajov	BL4
	24) princípy elektronickej pošty, vyhľadávacích/analytických techník, nástrojov a používania súborov cookies	BL4
	25) princípy webových služieb (napr. architektúra orientovaná na služby, protokol SOAP a jazyk HTML)	BL4
	26) princípy zálohovania a obnovy dát	BL4
	27) programovacie rozhrania pre prístup k databázam	BL4
	28) šifrovacie algoritmy pre lokálne bezdrôtové siete (WLAN)	BL4
	29) systémy riadenia bázy dát a ich správa, dopytovacie jazyky, relácie medzi tabuľkami	BL4
	30) štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch	BL5
	31) technológie filtrovania webového obsahu	BL5
	32) terminológia dátovej komunikácie (napr. sieťové protokoly, Ethernet, IP, šifrovanie, optické zariadenia, vymeniteľné médiá)	BL6
	33) typy sieťovej komunikácie (napr LAN, WAN, MAN, WLAN, WWAN)	BL6
	34) typy webových stránok, správa, funkcie a systémy na správu obsahu (CMS)	BL5
	35) XML schémy (Extensible Markup Language)	BL4
	36) koncepty kybernetických operácií, terminológia/slovník (t. j. príprava prostredia, kybernetický útok, kybernetická obrana), zásady, obmedzenia a účinky	BL6
	37) základy sieťovej a internetovej komunikácie (t. j. zariadenia, konfigurácia zariadení hardvér, softvér,	BL5

	aplikácie, porty/protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.)	
	38) princípy zraniteľností bezdrôtových sietí	BL5
	Riadenie hrozieb a rizík	
	1) procesy riadenia rizík, postupy a metodiky analýzy rizík	BL4
	2) typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie	BL4
	3) zásady aplikačnej bezpečnosti	BL4
	4) teória, koncepty a metódy systémového inžinierstva	BL4
	5) metódy a techniky softvérového inžinierstva vrátane modelov vývoja softvéru, princípy životného cyklu vývoja systémov a zásady bezpečného vývoja softvéru	BL4
	6) bezpečnostné koncepty v operačných systémoch	BL4
	7) bezpečnostné mechanizmy a metódy v softvérovom inžinierstve (napr. modularizácia, vrstvenie, abstrakcia, maskovanie, šifrovanie, pseudonymizácia, minimalizácia spracúvania atď.)	BL4
	8) techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť	BL4
	9) nástroje na posudzovanie zraniteľností	BL4
	10) sieťové protokoly a adresárové služby	BL4
	11) architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)	BL4
	12) prevádzka webových stránok (napr. webové servery, hosting, DNS, webové jazyky atď.)	BL4
	13) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL4*
	14) posudzovanie sieťových útokov a vzťahu jednotlivých typov sieťových útokov k hrozbám a zraniteľnostiam	BL4
	15) princípy a techniky etického hackingu	BL4
	16) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletiny)	BL4
	17) triedy a vektory útokov	BL4
	Aplikácia bezpečnostných opatrení	
	1) navrhovanie opatrení na ošetrenie bezpečnostných rizík	BL5
	2) bezpečnostné mechanizmy a spôsob ich implementácie	BL6
	3) bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti	BL3

	4) nástroje, metódy a techniky navrhovania bezpečnostných systémov	BL5
	5) zásady personálnej bezpečnosti	BL6
	6) opatrenia týkajúce sa používania, spracovania, uchovávania a prenosu údajov	BL5
	7) zásady a princípy riadenia identít a prístupov	BL4
	8) kryptografické bezpečnostné mechanizmy	BL4
	9) koncepcie a technológie vzdialeného prístupu	BL4
	10) virtualizačné technológie, vývoj a údržba virtuálnych strojov	BL4
	11) zabezpečenie virtuálnych privátnych sietí (VPN)	BL4
	12) techniky a metódy správy systémov a hardeningu systémov	BL4
	Výkon operatívnych bezpečnostných činností	
	1) procesy riešenia kybernetických bezpečnostných incidentov	BL5
	2) znalosti o štádiách kybernetického útoku (napr. prieskum, skenovanie, získanie prístupu, eskalácia oprávnení, využitie, zahladenie stôp)	BL5
	3) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia	BL5
	4) princípy logovania a bezpečnostného monitorovania	BL5
	5) princípy korelácie bezpečnostných udalostí	BL5
	6) identifikácia digitálnych stôp a postupy pri ich spracúvaní	BL4
	7) princípy, nástroje a techniky testovania prieniku	BL5
	8) analýza sieťového prenosu (nástroje, metodiky, procesy)	BL4
	9) bezdrôtové technológie (napr. celulárne, satelitné, GSM) zahŕňajúce základnú štruktúru, architektúru a dizajn moderných bezdrôtových komunikačných systémov	BL4
	10) charakteristiky komunikačných sietí (napr. kapacita, funkčnosť, trasy, kritické uzly)	BL4
	11) forenzné súvislosti štruktúry a procesov operačného systému	BL4
	12) koncepcia architektúry sietí vrátane topológie, protokolov, komponentov a bezpečnostných princípov	BL3
	13) požiadavky na vybavenie forenzných laboratórií a podporných aplikácií (napr. VMWare, Wireshark)	BL3
	14) mechanizmy zabezpečenia siete (napr. Host based IDS, IPS, ACL) vrátane ich funkcií a umiestnenia v sieti	BL4
	15) metódy a nástroje analýzy sieťového prenosu	BL4
	16) porty a služby operačných systémov	BL5

	17) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra)	BL5
	18) princípy hĺbkovej ochrany a architektúry sieťovej bezpečnosti	BL4
	19) princípy sieťových demilitarizovaných zón	BL4
	20) princípy súborových systémov (napr. NTFS, FAT a iné)	BL4
	21) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii	BL6
	22) bezpečnostné zásady správy a údržby databázových systémov	BL4
	23) zásady riadenia bezpečnosti prostredia cloudu	BL4
	24) základy digitálnej forenznej analýzy pri získavaní použiteľných informácií	BL3
	25) zásady riadenia sieťových systémov, modely, metódy (napr. monitorovanie výkonnosti systémov end-to-end)	BL5
	26) princípy zraniteľností bezdrôtových sietí	BL5
	Riadenie súladu	
	1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť	BL3
	2) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na ochranu osobných údajov	BL3
	3) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na prevádzku informačných a komunikačných technológií	BL3
	4) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky	BL3
	5) princípy posudzovania kybernetickej bezpečnosti	BL4
	6) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii	BL4
	7) základné metódy vyučovania a prezentovania (spôsob vyučovania a spôsob prípravy a vedenia prezentácií)	BL3
	8) štandardy bezpečnosti platobných kariet (PCI)	BL5*
	9) štandardy a procesy riadenia rizík v dodávateľskom reťazci	BL5
	10) metódy testovania a vyhodnocovania bezpečnosti systémov	BL5
Zručnosti:	**Riadenie bezpečnosti**	
	1) podpora riadenia informačnej a kybernetickej bezpečnosti organizácie	

	2) implementácia procesov informačnej a kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov 3) metodické usmerňovanie správcov a gestorov informačných a komunikačných technológií, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov vo vzťahu k dosahovaniu bezpečnostných cieľov organizácie 4) riadenie informačnej a kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri zaobstarávaní, projektovaní a vývoji softvéru a systémov 5) správa bezpečnosti informačných aktív organizácie **Riadenie hrozieb a rizík** 1) implementácia procesov a nástrojov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík 2) posudzovanie hrozieb a rizík a návrh opatrení na ošetrovanie rizík 3) hodnotenie technických zraniteľností systémov 4) detekcia, riešenie, evidencia a prevencia kybernetických bezpečnostných incidentov 5) podpora procesov obnovy prevádzkových činnosti (tzv. Business Continuity Management) vrátane riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning) **Aplikácia bezpečnostných opatrení** 1) zabezpečovanie implementácie zmien a optimalizácie technických a organizačných bezpečnostných opatrení 2) zabezpečovanie návrhov, zmien a integrácie bezpečnostných technológií a riešení 3) podpora riadenia bezpečnostnej architektúry 4) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie 5) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení **Výkon operatívnych bezpečnostných činností** 1) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe 2) aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov 3) prevádzka technických bezpečnostných opatrení

<table>
<tr><td></td><td colspan="3">4) zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov
5) riadenie projektov v kybernetickej bezpečnosti

Riadenie súladu
1) pravidelné preskúmavanie stavu kybernetickej a informačnej bezpečnosti
2) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti
3) zabezpečovanie školení zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti
4) budovanie bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov
5) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní</td></tr>
<tr><td>Stupeň vzdelania:</td><td>Úplné stredné všeobecné alebo úplné stredné odborné</td><td>Vysokoškolské I. stupňa</td><td>Vysokoškolské II. a III. stupňa</td></tr>
<tr><td>Odborná prax:</td><td>• najmenej 3 roky praxe v oblasti informačných technológií
• z toho najmenej 1 rok praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT</td><td>• najmenej 2 roky praxe v oblasti informačných technológií
• z toho najmenej 1 rok praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT</td><td>• najmenej 2 roky praxe v oblasti informačných technológií
• z toho najmenej 1 rok praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT</td></tr>
<tr><td>Špecifické kľúčové kompetencie</td><td colspan="3">a) schopnosť prijímať rozhodnutia
b) schopnosť myslieť a konať v súvislostiach
c) analytické myslenie
d) tvorivosť (kreativita)
e) prezentačná zručnosť
f) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí
g) schopnosť organizovania a plánovania práce
h) strategické a koncepčné myslenie</td></tr>
</table>

Požiadavky označené * sú odvetvovo závislé. Pre príslušnú rolu sú posudzované v kontexte kompetencií, potrebných na vykonávanie určitej pracovnej činnosti v konkrétnom odvetví.