Lektor kybernetickej bezpečnosti

Rola:	**Lektor kybernetickej bezpečnosti**	
Vedomosti:	**Riadenie bezpečnosti**	
	1) procesy, systémy a zásady riadenia informačnej a kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti	BL5
	2) zásady organizácie informačnej a kybernetickej bezpečnosti	BL5
	3) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti	BL5
	4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí	BL5
	5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI, metodiky merania vyspelosti atď.)	BL5
	6) zdroje, charakteristiky a použitie informačných aktív organizácie	BL5
	7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami	BL5
	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	BL5
	13) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.)	BL5
	14) zásady riadenia dodávateľských služieb a obstarávania informačných systémov vrátane vyhodnocovania dôveryhodnosti dodávateľa alebo výrobku	BL5
	15) charakteristiky fyzických a virtuálnych nosičov údajov	BL5
	16) elektrotechnika aplikovaná na architektúru počítačov (napr. základné dosky, procesory, čipy a iný počítačový hardvér)	BL5
	17) koncepcia a mechanizmy zálohovania a obnovy dát	BL5
	18) kryptografické algoritmy	BL5

	19) kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy a steganografia)	BL5
	20) kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov	BL5
	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 cookie	BL6
	25) princípy webových služieb (napr. architektúra orientovaná na služby, protokol SOAP a jazyk HTML)	BL6
	26) princípy zálohovania a obnovy dát	BL6
	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, tabuľkové vzťahy	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, aplikácie, porty/protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.)	BL5
	38) princípy zraniteľností bezdrôtových sietí	BL5
	Riadenie hrozieb a rizík	
	1) procesy riadenia rizík, postupy a metodiky analýzy rizík	BL5
	2) typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie	BL5
	3) zásady aplikačnej bezpečnosti	BL6
	4) teória, koncepty a metódy systémového inžinierstva	BL5

	5) metódy a techniky softvérového inžinierstva vrátane modelov vývoja softvéru, princípy životného cyklu vývoja systémov a zásady bezpečného vývoja softvéru	BL5
	6) bezpečnostné koncepty v operačných systémoch	BL5
	7) bezpečnostné mechanizmy a metódy v softvérovom inžinierstve (napr. modularizácia, vrstvenie, abstrakcia, maskovanie, šifrovanie, pseudonymizácia, minimalizácia spracúvania atď.)	BL5
	8) techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť	BL5
	9) nástroje na posudzovanie zraniteľností	BL5
	10) sieťové protokoly a adresárové služby	BL5
	11) architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)	BL5
	12) prevádzka webových stránok (napr. webové servery, hosting, DNS, webové jazyky atď.)	BL6
	13) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL5*
	14) posudzovanie sieťových útokov a vzťahu jednotlivých typov sieťových útokov k hrozbám a zraniteľnostiam	BL5
	15) princípy a techniky etického hackingu	BL5
	16) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletiny)	BL5
	17) triedy a vektory útokov	BL5
	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	BL5
	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	BL5
	8) kryptografické bezpečnostné mechanizmy	BL5
	9) koncepcie a technológie vzdialeného prístupu	BL5
	10) virtualizačné technológie, vývoj a údržba virtuálnych strojov	BL5
	11) zabezpečenie virtuálnych privátnych sietí (VPN)	BL5

	12) techniky a metódy správy systémov a hardeningu systémov	BL5
	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) konfigurácia 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 Windows/Unix	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	BL5
	19) princípy sieťových demilitarizovaných zón	BL5
	20) princípy súborových systémov (napr. NTFS, FAT a iné)	BL5
	21) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii	BL6
	22) bezpečnostné zásady správy a údržby databázových systémov	BL5
	23) zásady riadenia bezpečnosti prostredia cloudu	BL5

	24) základy digitálnej forenznej analýzy pri získavaní použiteľných informácií	BL4
	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) zásady a metódy tvorby učebných plánov, výuky jednotlivcov a skupín	BL4
	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:	a) znalosť metód výuky b) znalosť systémov riadenia vzdelávania a ich využitie pri riadení vzdelávania c) znalosť úrovní vzdelávacích cieľov (t. j. Bloomova taxonómia) d) znalosť štýlov výuky e) schopnosť pripraviť a prezentovať lekcie f) schopnosť pripravovať a poskytovať informácie s cieľom zabezpečiť, aby si používatelia systémov, sietí a údajov boli vedomí a dodržiavali zásady a postupy zabezpečenia systémov g) schopnosť aplikovať princípy vzdelávania dospelých h) schopnosť merať úroveň vedomostí študentov a procesov testovania a hodnotenia študentov i) znalosť princípov a procesov vykonávania hodnotenia potrieb odbornej prípravy a vzdelávania j) schopnosť poskytnúť študentom účinnú spätnú väzbu na zlepšenie výučby	

	k) schopnosť rozvíjať alebo obstarávať učebné osnovy, ktoré sa venujú téme na primeranej úrovni pre daný cieľ l) schopnosť rozvíjať učebné osnovy pre použitie vo virtuálnom prostredí m) schopnosť rozvíjať učebné osnovy, ktoré sa venujú danej téme na primeranej úrovni pre cieľové publikum n) schopnosť vykonávať hodnotenie potrieb odbornej prípravy a vzdelávania o) schopnosť vyvinúť inštruktážne materiály p) znalosť systémov počítačových školení a e-learningových služieb q) znalosť zásad a metód odbornej prípravy a výučby pri tvorbe učebných plánov, výučbe a výučbe pre jednotlivcov a skupiny a meraní účinkov odbornej prípravy a vzdelávania r) zručnosť používania technológií výuky (napr. webových stránok, počítačov, projektorov) na účely výučby s) schopnosť graficky znázorniť materiály na podporu vzdelávania t) zručnosť pri využívaní a rozvíjaní vzdelávacích aktivít (napr. scenáre, inštruktážne hry, interaktívne cvičenia) u) zručnosť pri vývoji a vykonávaní programov technického vzdelávania a učebných osnov v) schopnosť komunikovať komplexné informácie, koncepty alebo návrhy dôveryhodnými verbálnymi, písomnými a/alebo vizuálnymi prostriedkami w) znalosti o technikách a metódach výroby, komunikácie a šírenia informácií vrátane alternatívnych spôsobov informovania prostredníctvom písomných, ústnych a vizuálnych médií x) zručnosť pri využívaní virtuálnych pracovných priestorov a/alebo nástrojov na spoluprácu (chatovacie miestnosti, SharePoint)
Špecifické kľúčové kompetencie	a) prezentačná zručnosť b) analytické myslenie c) tvorivosť (kreativita) d) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí e) schopnosť organizovania a plánovania práce