

ZBIERKA ZÁKONOV SLOVENSKEJ REPUBLIKY

Ročník 2022

Vyhlásené: 23. 12. 2022

Časová verzia predpisu účinná od: 1. 1.2024

Obsah dokumentu je právne záväzný.

492

VYHLÁŠKA

Národného bezpečnostného úradu

z 19. decembra 2022,

**ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej
bezpečnosti**

Národný bezpečnostný úrad podľa § 32 ods. 1 písm. d) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1

Táto vyhláška ustanovuje znalostné štandardy v oblasti kybernetickej bezpečnosti (ďalej len „znalostný štandard“) prostredníctvom jednotlivých rolí kybernetickej bezpečnosti (ďalej len „rola“). Znalostné štandardy sú určené na preukazovanie minimálnych požiadaviek na výkon konkrétnej roly a budovanie bezpečnostného povedomia.

§ 2

(1) Konkrétna činnosť, ktorou osoba vykonáva úlohy a činnosti podľa zákona, je určená prostredníctvom konkrétnej roly, v ktorej osoba vystupuje vo vzťahu k sieti alebo k informačnému systému.

(2) Charakteristika vzdelávacích potrieb pre jednotlivé kategórie používateľov informačno-komunikačných technológií je uvedená v prílohe č. 1 a úrovne vzdelávacích cieľov sú uvedené v prílohe č. 2.

(3) Znalostné štandardy pre konkrétnu rolu sú uvedené v prílohách č. 3 až 14.

(4) Znalostné štandardy pre určitú rolu sú splnené aj kolektívne ich vzájomným zdieľaním. Tvorba názvov pracovných pozícií a ich pracovných náplní sa určuje prevádzkovateľom základnej služby.

§ 3

Táto vyhláška nadobúda účinnosť 1. januára 2023 okrem príloh č. 3 až 5 a príloh č. 7 až 14, ktoré nadobúdajú účinnosť 1. januára 2024.

Roman Konečný v. r.

Príloha č. 1
k vyhláške č. 492/2022 Z. z.

Charakteristika vzdelávacích potrieb

Kategória používateľov	Popis kategórie používateľov	Cieľ vzdelávania pre príslušnú kategóriu
laik	používateľ IKT okrem výkonu konkrétneho povolania	a) porozumieť vybraným základným pojmom kybernetickej bezpečnosti, b) porozumieť významu osobných údajov a citlivých informačných aktív v mimopracovnej oblasti a osvojiť si základné pravidlá bezpečnej manipulácie a používania IKT.
odborný zamestnanec	používateľ, ktorý pri výkone povolania využíva sieť alebo informačný systém	a) porozumieť vybraným základným pojmom kybernetickej bezpečnosti, b) porozumieť svojej úlohe a zodpovednosti v systéme kybernetickej bezpečnosti, c) chápať význam informačných aktív s ktorými zamestnanec pracuje, d) porozumieť potrebe ochrany informácií a informačných aktív, e) osvojiť si základné pravidlá bezpečnej práce s IKT, f) rozpoznať incident a vedieť naň správne reagovať, g) porozumieť bezpečnostným politikám a používaniu bezpečnostných mechanizmov v pracovných procesoch.
manažér	riadiaci zamestnanec, ktorý nie je IT manažérom alebo manažérom kybernetickej bezpečnosti a ktorý spravidla zodpovedá za príslušný proces alebo skupinu procesov a v rámci nich zodpovedá aj za plnenie úloh v oblasti riadenia rizík kybernetickej bezpečnosti	a) porozumieť vybraným základným pojmom kybernetickej bezpečnosti, b) porozumieť rizikám kybernetickej bezpečnosti v riadených procesoch, c) nadobudnúť schopnosť analyzovať požadovanú úroveň ochrany informačných aktív, d) nadobudnúť schopnosť integrovať požiadavky kybernetickej bezpečnosti do procesov a úloh podriadených zamestnancov, e) naučiť sa definovať a dohliadať na plnenie požiadaviek kybernetickej bezpečnosti pri obstaraní produktov a služieb a pri procesoch podporovaných tretími stranami.
IT manažér	riadiaci zamestnanec organizačných jednotiek zodpovedných za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie prostriedkov IKT	a) porozumieť významu kybernetickej bezpečnosti pre činnosť organizácie, b) poznať jednotlivé oblasti kybernetickej bezpečnosti, c) porozumieť systému riadenia bezpečnosti informácií a informačných aktív a osvojiť si ho, d) nadobudnúť schopnosť implementovať bezpečnostné opatrenia v konkrétnom prostredí,

		e) nadobudnúť schopnosť určiť zodpovednosti zamestnancov organizácie vo vzťahu k informačným a komunikačným technológiám, f) osvojiť si metódy vyhodnocovania efektívnosti prijatých bezpečnostných opatrení, g) vedieť definovať a kontrolovať plnenie požiadaviek kybernetickej bezpečnosti pri obstarávaní, dodávaní, správe, prevádzke, údržbe a rozvoji sietí a informačných systémov a ich komponentov, h) nadobudnúť schopnosť presadzovať politiky kybernetickej bezpečnosti v organizácii.
informatik	zamestnanec zodpovedný za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie IKT	a) doplniť vlastné odborné znalosti špecificky pre oblasť kybernetickej bezpečnosti, b) porozumieť podstate bezpečnostných požiadaviek na IKT a IT služby, c) porozumieť zraniteľnostiam, hrozbám a rizikám spojeným s používanými IKT a IT službami, d) nadobudnúť schopnosť navrhnuť, implementovať, udržiavať a prevádzkovať mechanizmy na naplnenie bezpečnostných požiadaviek na IKT a IT služby, e) nadobudnúť zručnosť kvalifikovane komunikovať a spolupracovať so špecialistami kybernetickej bezpečnosti, formulovať problémy, posudzovať a implementovať navrhované opatrenia.
zamestnanec v kybernetickej bezpečnosti	zamestnanec špecializovaný na oblasť bezpečnosti informácií a riadenia rizík kybernetickej bezpečnosti, zodpovedný za návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie bezpečnostných mechanizmov a riešení	a) poznať a osvojiť si právne a etické požiadavky na zaručenie bezpečnosti informačných aktív, b) rozumieť zraniteľnostiam, hrozbám a rizikám v informačnej a kybernetickej bezpečnosti, c) nadobudnúť schopnosť navrhnuť, implementovať, udržiavať a prevádzkovať bezpečnostné mechanizmy a riešenia, d) nadobudnúť schopnosť navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru, e) nadobudnúť znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a uplatňovať ich v procesoch organizácie, f) nadobudnúť zručnosť kvalifikovane komunikovať a spolupracovať s informatikmi, formulovať problémy, posudzovať a implementovať navrhované opatrenia, g) nadobudnúť schopnosť navrhovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti.

manažér kybernetickej bezpečnosti	riadiaci zamestnanec špecializovaný na oblasť bezpečnosti informácií a riadenia rizík kybernetickej bezpečnosti, vlastníci bezpečnostných procesov	a) nadobudnúť schopnosť vytvoriť rámec riadenia kybernetickej bezpečnosti v organizácii, b) nadobudnúť schopnosť riadiť procesy súvisiace s informačnou a kybernetickou bezpečnosťou v organizácii, c) nadobudnúť schopnosť formulovať návrhy a odporúčania na obstaranie, implementáciu, prevádzku a vyhodnocovanie bezpečnostných mechanizmov a riešení a navrhovať a manažovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti, d) nadobudnúť schopnosť navrhovať, implementovať, udržiavať a prevádzkovať bezpečnostné mechanizmy a riešenia, e) nadobudnúť znalosti o právnych a etických požiadavkách na zaručenie bezpečnosti informačných aktív, f) nadobudnúť schopnosť navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru, g) nadobudnúť a osvojiť si znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a schopnosť uplatňovať ich v procesoch organizácie, h) nadobudnúť schopnosti pri presadzovaní bezpečnostných opatrení.
auditor a výskumník kybernetickej bezpečnosti	odborný zamestnanec špecializovaný na oblasť výskumu alebo posudzovania kybernetickej bezpečnosti, analýzy rizík, testovania a vyhodnocovania efektivity bezpečnostných opatrení, posudzovania zhody a súladu	a) nadobudnúť schopnosti v rozsahu podľa predchádzajúcich cieľov platných pre všetky ostatné kategórie, b) vykonať audit kybernetickej bezpečnosti a posúdiť efektívnosť prijatých bezpečnostných opatrení podľa vyhlášky Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora a platných auditných metódik.

Príloha č. 2
k vyhláške č. 492/2022 Z. z.

Úrovně vzdelávacích cieľov

1. Kvalifikačné štandardy pre kybernetickú bezpečnosť podľa tejto vyhlášky majú šesť úrovní vzdelávacích cieľov charakterizované opisnými prvkami v jazyku všeobecných nárokov na vzdelávacie výstupy vo vzťahu k vedomostiam, zručnostiam a kompetenciám, ktoré zodpovedajú kvalifikácii na danej úrovni kvalifikačného rámca.
2. Triedenie vzdelávacích cieľov je sekvenčné a zároveň kumulatívne; pre dosiahnutie vyššieho vzdelávacieho cieľa je potrebné dosiahnuť všetky predchádzajúce vzdelanostné úrovne.

Úroveň	Vzdelávací cieľ	Popis vzdelávacieho cieľa
BL1	ZAPAMÄTANIE	Schopnosť zapamätať si potrebné informácie. Skúšobné otázky spojené s touto úrovňou testujú pamäť uchádzača a zahŕňajú úlohy ako: definícia, výber zo zoznamu, rozpoznanie, popis a pomenovanie.
BL2	POCHOPENIE	Schopnosť porozumieť alebo pochopiť význam toho, čo bolo komunikované a využiť získanú informáciu bez toho, aby ju uchádzač spájal s inými informáciami, interpretáciami alebo materiálmi. Otázky na preskúmanie vedomostí na tejto úrovni zahŕňajú scenáre, ktoré uvádzajú príklady, ilustrácie, odvodenia, sumarizáciu a interpretáciu. Úroveň zahŕňa vedomosti získané na predchádzajúcej úrovni.
BL3	APLIKÁCIA	Uchádzač je schopný používať myšlienky, princípy a teórie v nových, konkrétnych situáciách. Otázky na preskúmanie na tejto úrovni zahŕňajú vedomosti a pochopenie a môžu zahŕňať úlohy typu: výber vhodných postupov, uplatňovanie zásad, použitie prístupu alebo identifikácia možností. Úroveň zahŕňa vedomosti získané na predchádzajúcich úrovniach.
BL4	ANALÝZA	Uchádzač je schopný rozdeliť komunikáciu na základné časti, aby bol jasne uchopený význam informácie. V tejto úrovni sa skúma podstata jednotlivých entít, s cieľom lepšie porozumieť komplexným celkom. Úroveň zahŕňa vedomosti získané na predchádzajúcich úrovniach.
BL5	SYNTEZA	Na tejto úrovni je uchádzač schopný opätovne spojiť rôzne časti alebo prvky konceptu do jednotného systému alebo celku. Toto

		spojenie a zmysel pre malé časti je rozhodujúcim faktorom v učení. Úroveň vzdelávania BL5 je pre uchádzača typicky najintenzívnejšia. Otázky na preskúmanie vedomostí na tejto úrovni zahŕňajú scenáre ako: tvorba, návrh, písanie, kombinovanie, skladanie, organizovanie, revízia a plánovanie. Úroveň zahŕňa vedomosti získané na predchádzajúcich úrovniach.
BL6	POSÚDENIE	Na tejto úrovni je uchádzač schopný dospieť k prehľadu a posúdiť hodnotu a relatívny prínos myšlienok alebo postupov pomocou vhodných kritérií. Uchádzač je schopný porovnávať, posudzovať, hodnotiť, odôvodňovať, kritizovať a využitím dialektických postupov spochybňovať teórie, postupy, metódy a koncepty. Úroveň zahŕňa vedomosti získané na všetkých predchádzajúcich úrovniach.

Príloha č. 3
k vyhláške č. 492/2022 Z. z.

Odborný zamestnanec

Rola:	Odborný zamestnanec																																		
Vedomosti:	<table border="0"> <tr> <td>1) vybrané základné pojmy v kybernetickej bezpečnosti</td><td>BL2</td></tr> <tr> <td>2) význam osobných údajov a citlivých informačných aktív</td><td>BL2</td></tr> <tr> <td>3) zdroje typických hrozieb a kategórie hrozieb (úmyselné hrozby, náhodné hrozby, hrozby prostredia)</td><td>BL2</td></tr> <tr> <td>4) aktuálne typy hrozieb (napr. škodlivý kód, phishing, spam, útok na internetové služby alebo stránky (Denial of Service (DoS)/znemožnenie prístupu k požadovanej službe (Distributed denial of service (DDoS), botnety, krádež identity a ďalšie)</td><td>BL2</td></tr> <tr> <td>5) identifikácia, autentizácia, autorizácia</td><td>BL2</td></tr> <tr> <td>6) spôsoby overenia digitálnej totožnosti význam viacfaktorovej autentizácie a typy autentizačných faktorov</td><td>BL2</td></tr> <tr> <td>7) základné princípy bezpečného používania hesiel</td><td>BL2</td></tr> <tr> <td>8) význam škodlivého kódu (malvér) a spôsoby útokov škodlivým kódom</td><td>BL2</td></tr> <tr> <td>9) riziká používania zariadení IKT</td><td>BL2</td></tr> <tr> <td>10) základné zraniteľnosti smartfónov</td><td>BL2</td></tr> <tr> <td>11) základné princípy vzdialeného prístupu a bezpečnostné zásady pri práci na diaľku</td><td>BL2</td></tr> <tr> <td>12) obsah pojmu digitálne súkromie</td><td>BL2</td></tr> <tr> <td>13) význam pojmov digitálny popis, elektronický podpis, kvalifikovaný elektronický podpis, časová pečiatka</td><td>BL2</td></tr> <tr> <td>14) základné zásady bezpečnosti, ochrany osobných údajov a etikety pri telekonferenciách a online rokovaníach, stretnutiach</td><td>BL2</td></tr> <tr> <td>15) bezpečnostné riziká a riziká ochrany súkromia pri používaní sociálnych sietí pokiaľ sú v organizácii povolené</td><td>BL2</td></tr> <tr> <td>16) podstata útokov formou sociálneho inžinierstva (phishing, vishing, smishing, Business Email Compromise)</td><td>BL2</td></tr> <tr> <td>17) základné poznatky na úseku trestného práva</td><td>BL2</td></tr> </table>	1) vybrané základné pojmy v kybernetickej bezpečnosti	BL2	2) význam osobných údajov a citlivých informačných aktív	BL2	3) zdroje typických hrozieb a kategórie hrozieb (úmyselné hrozby, náhodné hrozby, hrozby prostredia)	BL2	4) aktuálne typy hrozieb (napr. škodlivý kód, phishing, spam, útok na internetové služby alebo stránky (Denial of Service (DoS)/znemožnenie prístupu k požadovanej službe (Distributed denial of service (DDoS), botnety, krádež identity a ďalšie)	BL2	5) identifikácia, autentizácia, autorizácia	BL2	6) spôsoby overenia digitálnej totožnosti význam viacfaktorovej autentizácie a typy autentizačných faktorov	BL2	7) základné princípy bezpečného používania hesiel	BL2	8) význam škodlivého kódu (malvér) a spôsoby útokov škodlivým kódom	BL2	9) riziká používania zariadení IKT	BL2	10) základné zraniteľnosti smartfónov	BL2	11) základné princípy vzdialeného prístupu a bezpečnostné zásady pri práci na diaľku	BL2	12) obsah pojmu digitálne súkromie	BL2	13) význam pojmov digitálny popis, elektronický podpis, kvalifikovaný elektronický podpis, časová pečiatka	BL2	14) základné zásady bezpečnosti, ochrany osobných údajov a etikety pri telekonferenciách a online rokovaníach, stretnutiach	BL2	15) bezpečnostné riziká a riziká ochrany súkromia pri používaní sociálnych sietí pokiaľ sú v organizácii povolené	BL2	16) podstata útokov formou sociálneho inžinierstva (phishing, vishing, smishing, Business Email Compromise)	BL2	17) základné poznatky na úseku trestného práva	BL2
1) vybrané základné pojmy v kybernetickej bezpečnosti	BL2																																		
2) význam osobných údajov a citlivých informačných aktív	BL2																																		
3) zdroje typických hrozieb a kategórie hrozieb (úmyselné hrozby, náhodné hrozby, hrozby prostredia)	BL2																																		
4) aktuálne typy hrozieb (napr. škodlivý kód, phishing, spam, útok na internetové služby alebo stránky (Denial of Service (DoS)/znemožnenie prístupu k požadovanej službe (Distributed denial of service (DDoS), botnety, krádež identity a ďalšie)	BL2																																		
5) identifikácia, autentizácia, autorizácia	BL2																																		
6) spôsoby overenia digitálnej totožnosti význam viacfaktorovej autentizácie a typy autentizačných faktorov	BL2																																		
7) základné princípy bezpečného používania hesiel	BL2																																		
8) význam škodlivého kódu (malvér) a spôsoby útokov škodlivým kódom	BL2																																		
9) riziká používania zariadení IKT	BL2																																		
10) základné zraniteľnosti smartfónov	BL2																																		
11) základné princípy vzdialeného prístupu a bezpečnostné zásady pri práci na diaľku	BL2																																		
12) obsah pojmu digitálne súkromie	BL2																																		
13) význam pojmov digitálny popis, elektronický podpis, kvalifikovaný elektronický podpis, časová pečiatka	BL2																																		
14) základné zásady bezpečnosti, ochrany osobných údajov a etikety pri telekonferenciách a online rokovaníach, stretnutiach	BL2																																		
15) bezpečnostné riziká a riziká ochrany súkromia pri používaní sociálnych sietí pokiaľ sú v organizácii povolené	BL2																																		
16) podstata útokov formou sociálneho inžinierstva (phishing, vishing, smishing, Business Email Compromise)	BL2																																		
17) základné poznatky na úseku trestného práva	BL2																																		
Zručnosti:	<table border="0"> <tr> <td>1) bezpečná manipulácia s prostriedkami IKT, osobnými údajmi a citlivými informačnými aktívami</td><td></td></tr> <tr> <td>2) používanie stanovených bezpečnostných mechanizmov v pracovných procesoch</td><td></td></tr> <tr> <td>3) rozpoznanie bezpečnostného incidentu a schopnosť správne reagovať na incident</td><td></td></tr> <tr> <td>4) dodržiavanie bezpečnostných zásad a platných politík</td><td></td></tr> </table>	1) bezpečná manipulácia s prostriedkami IKT, osobnými údajmi a citlivými informačnými aktívami		2) používanie stanovených bezpečnostných mechanizmov v pracovných procesoch		3) rozpoznanie bezpečnostného incidentu a schopnosť správne reagovať na incident		4) dodržiavanie bezpečnostných zásad a platných politík																											
1) bezpečná manipulácia s prostriedkami IKT, osobnými údajmi a citlivými informačnými aktívami																																			
2) používanie stanovených bezpečnostných mechanizmov v pracovných procesoch																																			
3) rozpoznanie bezpečnostného incidentu a schopnosť správne reagovať na incident																																			
4) dodržiavanie bezpečnostných zásad a platných politík																																			

Príloha č. 4
k vyhláške č. 492/2022 Z. z.

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)	konceptia 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, bulletin)	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 objektivej bezpečnosti	BL3

4) nástroje, metódy a techniky navrhovania bezpečnostných systémov	BL5
5) zásady personálnej bezpečnosti	BL6
6) opatrenia týkajúce sa používania, spracovania, uchovávaní 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 činností (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
--	---

	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		
Stupeň vzdelania:	Úplné stredné všeobecné alebo úplné stredné odborné	Vysokoškolské I. stupňa	Vysokoškolské II. a III. stupňa
Odborná prax:	- 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	- 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	- 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
Špecifické kľúčové kompetencie	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		

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

Príloha č. 5
k vyhláške č. 492/2022 Z. z.

Manažér kybernetickej bezpečnosti

Rola:	Manažér kybernetickej bezpečnosti
Vedomosti:	Riadenie bezpečnosti 1) procesy, systémy a zásady riadenia kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti BL5 2) organizácia kybernetickej bezpečnosti BL6 3) terminológia a skratky v oblasti kybernetickej bezpečnosti BL6 4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí BL5 5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI atď.) BL5 6) zdroje, charakteristiky a použitie informačných aktív organizácie BL6 7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami BL6 8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI) BL6 9) zásady a techniky plánovania kapacity a plánovania zdrojov BL5 10) princípy riadenia ľudských zdrojov BL6 11) rozpočtové pravidlá, zásady plánovania a riadenia nákladov a plánovania a riadenia investícií BL5 12) základy compliance v oblasti kybernetickej bezpečnosti (právny rámec aspoň na úrovni zákona o ITVS, GDPR, ePrivacy, ISO 20000) BL3 13) výskumné stratégie a znalostný manažment BL4 14) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.) BL5 15) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) BL4 16) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly BL5 17) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.) BL2

18) zásady riadenia dodávateľských služieb a obstarávania informačných systémov vrátane vyhodnocovania dôveryhodnosti dodávateľa alebo výrobku	BL6
Riadenie hrozieb a rizík	
1) procesy riadenia rizík, postupy a metodiky analýzy rizík	BL6
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.)	BL5
8) techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť	BL3
9) nástroje na posudzovanie zraniteľností	BL3
10) sieťové protokoly a adresárové služby	BL3
11) základná architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)	BL3
12) bezpečnostné riziká cloud computingu	BL4
13) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL5*
Aplikácia bezpečnostných opatrení	
1) princípy navrhovania opatrení na ošetrovanie bezpečnostných rizík	BL6
2) bezpečnostné mechanizmy a spôsob ich implementácie	BL3
3) bezpečnostné opatrenia vo fyzickej a objektivej bezpečnosti	BL4
4) nástroje, metódy a techniky navrhovania bezpečnostných systémov	BL4
5) zásady personálnej bezpečnosti	BL5
6) opatrenia týkajúce sa používania, spracúvania, uchovávanía a prenosu údajov	BL6
7) zásady a princípy riadenia identít a prístupov	BL4
8) základy kryptografických bezpečnostných mechanizmov	BL4

9) koncepcie a technológie vzdialeného prístupu	BL4
10) základy virtualizačných technológií, vývoja a údržby virtuálnych strojov	BL3
11) princípy zabezpečenia virtuálnych privátnych sietí (VPN)	BL3
12) techniky a metódy správy systémov a hardeningu systémov	BL3
Výkon operatívnych bezpečnostných činností	
1) procesy riešenia kybernetických bezpečnostných incidentov	BL6
2) zásady riadenia bezpečnosti prostredia cloudu	BL5
3) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia	BL4
4) princípy logovania a bezpečnostného monitorovania	BL4
5) princípy korelácie bezpečnostných udalostí	BL4
6) základné postupy pri spracovaní digitálnych stôp	BL4
7) základy penetračného testovania	BL3
Riadenie súladu	
1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť a ochranu osobných údajov	BL6
2) základy compliance v oblasti kybernetickej bezpečnosti (právny rámec aspoň na úrovni zákona o ITVS, GDPR, ePrivacy, ISO 20000)	BL3
3) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky	BL6
4) princípy posudzovania kybernetickej bezpečnosti	BL5
5) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii	BL6
6) systémy odbornej prípravy, princípy vzdelávacích stratégií, procesov a postupov vzdelávania a zvyšovania povedomia u dospelých v oblasti kybernetickej bezpečnosti vrátane merania efektivity vzdelávania	BL6
7) zásady a metódy tvorby učebných plánov, výuky jednotlivcov a skupín	BL6
8) štandardy bezpečnosti platobných kariet (PCI)	BL4*
9) štandardy a procesy riadenia rizík v dodávateľskom reťazci	BL6
10) metódy testovania a vyhodnocovania bezpečnosti systémov	BL4

Zručnosti:	Riadenie bezpečnosti 1) strategické riadenie kybernetickej bezpečnosti organizácie 2) vypracovanie a prezentácia bezpečnostných stratégií a konceptov 3) implementácia a riadenie procesov kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov 4) zabezpečenie, vypracovanie, udržiavanie a aktualizácie bezpečnostnej dokumentácie kybernetickej bezpečnosti a ďalších interných riadiacich aktov vo vzťahu k bezpečnosti organizácie 5) návrh požiadaviek na rozpočet a na iné zdroje súvisiace s bezpečnostnými opatreniami a procesmi relevantnými z hľadiska kybernetickej bezpečnosti vrátane riadenia nákladov a riadenia investícií 6) 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 7) poskytovanie informácií bezpečnostnému výboru alebo štatutárnemu orgánu o stave kybernetickej bezpečnosti v organizácii, o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach 8) riadenie kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri obstarávaní a vývoji softvéru a systémov Riadenie hrozieb a rizík 1) implementácia a manažment procesov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík 2) posudzovanie hrozieb a rizík 3) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí 4) zabezpečovanie procesov hodnotenia technických zraniteľností systémov 5) manažment procesov detekcie, riešenia, evidencie a prevencie kybernetických bezpečnostných incidentov 6) zabezpečenie funkčných plánov kontinuity a obnovy činností organizácie 7) koordinácia a riadenie procesov obnovy prevádzkových činností (tzv. Business Continuity Management) vrátane riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning) Aplikácia bezpečnostných opatrení
------------	--

	1) riadenie návrhov, implementácie, zmien a optimalizácie bezpečnostných riešení s víziou a konceptom ich bežného prevádzkovania 2) zabezpečovanie implementácie technických a organizačných bezpečnostných opatrení 3) riadenie 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) manažment výkonu činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe 2) vedenie tímu zamestnancov útvaru informačnej a kybernetickej bezpečnosti, ak je taký organizačný útvar zriadený 3) návrh a aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov 4) riadenie bežnej prevádzky technických bezpečnostných opatrení 5) zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov 6) zaistenie uplatňovania princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie 7) základy projektového manažmentu
	Riadenie súladu 1) riadenie procesov zaručenia súladu (Compliance Management) v oblasti kybernetickej bezpečnosti 2) zabezpečenie pravidelného preskúmavania stavu kybernetickej a informačnej bezpečnosti 3) vyhodnocovanie plnenia vnútorných predpisov súvisiacich s riadením kybernetickej bezpečnosti 4) poskytovanie súčinnosti internému a externému auditu kybernetickej bezpečnosti 5) navrhovanie metrík a kľúčových indikátorov pre sledovanie vývoja a stavu bezpečnosti a vývoja bezpečnostných rizík 6) zabezpečovanie školení zamestnancov v oblasti kybernetickej bezpečnosti 7) zabezpečovanie kontinuálneho vzdelávania pre pracovné roly relevantné z hľadiska kybernetickej bezpečnosti 8) zabezpečovanie budovania bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov

	9) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní		
Stupeň vzdelania:	Úplné stredné všeobecné alebo úplné stredné odborné	Vysokoškolské I. stupňa	Vysokoškolské II. a III. stupňa
Odborná prax:	- najmenej 7 rokov praxe v oblasti informačných technológií - z toho najmenej 5 rokov praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok	- najmenej 5 rokov praxe v oblasti informačných technológií - z toho najmenej 3 roky praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok	- 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 - medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) schopnosť riešiť konflikty d) schopnosť poskytovať spätnú väzbu e) schopnosť delegovať úlohy f) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí g) schopnosť viesť pracovný tím h) schopnosť organizovania a plánovania práce i) analytické myslenie j) strategické a koncepčné myslenie k) tvorivosť (kreativita) l) prezentačná zručnosť		

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

Príloha č. 6
k vyhláške č. 492/2022 Z. z.

Audítor kybernetickej bezpečnosti

Rola:	Audítor kybernetickej bezpečnosti																																																				
Vedomosti:	<table border="0"> <tr><td>1) procesy a systémy riadenia informačnej a kybernetickej bezpečnosti</td><td>BL6</td></tr> <tr><td>2) zásady organizácie informačnej a kybernetickej bezpečnosti</td><td>BL6</td></tr> <tr><td>3) zásady personálnej bezpečnosti</td><td>BL6</td></tr> <tr><td>4) zásady riadenia prístupov a identít</td><td>BL6</td></tr> <tr><td>5) spôsob používania kryptografických bezpečnostných mechanizmov</td><td>BL6</td></tr> <tr><td>6) princípy testovania kybernetickej bezpečnosti</td><td>BL6</td></tr> <tr><td>7) zásady auditu kybernetickej bezpečnosti</td><td>BL6</td></tr> <tr><td>8) právne predpisy, požiadavky na súlad a normy vzťahujúce sa na kybernetickú bezpečnosť</td><td>BL6</td></tr> <tr><td>9) právne predpisy a požiadavky na súlad vzťahujúce sa na ochranu osobných údajov</td><td>BL6</td></tr> <tr><td>10) štandardy a zásady ochrany osobných údajov vrátane metodických usmernení Úradu na ochranu osobných údajov Slovenskej republiky</td><td>BL6</td></tr> <tr><td>11) procesy a metodiky riadenia rizík</td><td>BL6</td></tr> <tr><td>12) postupy analýzy rizík</td><td>BL6</td></tr> <tr><td>13) typické hrozby a postupy pre identifikáciu hrozieb a zraniteľností</td><td>BL6</td></tr> <tr><td>14) bezpečnostné mechanizmy</td><td>BL6</td></tr> <tr><td>15) metodiky podnikovej architektúry</td><td>BL6</td></tr> <tr><td>16) procesy riešenia kybernetických bezpečnostných incidentov</td><td>BL6</td></tr> <tr><td>17) princípy plánovania havarijnej obnovy prevádzky</td><td>BL6</td></tr> <tr><td>18) procesy riadenia kontinuity činností a princípov plánovania havarijnej obnovy</td><td>BL6</td></tr> <tr><td>19) princípy logovania a bezpečnostného monitorovania</td><td>BL6</td></tr> <tr><td>20) zásady riadenia fyzickej a objektovej bezpečnosti</td><td>BL6</td></tr> <tr><td>21) bezpečnostné mechanizmy vo fyzickej a objektovej bezpečnosti</td><td>BL6</td></tr> <tr><td>22) princípy riadenia služieb v oblasti informačných technológií</td><td>BL6</td></tr> <tr><td>23) princípy riadenia nákladov a rozpočtových pravidiel</td><td>BL6</td></tr> <tr><td>24) princípy riadenia ľudských zdrojov</td><td>BL6</td></tr> <tr><td>25) koncepty počítačových sietí</td><td>BL6</td></tr> <tr><td>26) zásady riadenia projektov</td><td>BL6</td></tr> </table>	1) procesy a systémy riadenia informačnej a kybernetickej bezpečnosti	BL6	2) zásady organizácie informačnej a kybernetickej bezpečnosti	BL6	3) zásady personálnej bezpečnosti	BL6	4) zásady riadenia prístupov a identít	BL6	5) spôsob používania kryptografických bezpečnostných mechanizmov	BL6	6) princípy testovania kybernetickej bezpečnosti	BL6	7) zásady auditu kybernetickej bezpečnosti	BL6	8) právne predpisy, požiadavky na súlad a normy vzťahujúce sa na kybernetickú bezpečnosť	BL6	9) právne predpisy a požiadavky na súlad vzťahujúce sa na ochranu osobných údajov	BL6	10) štandardy a zásady ochrany osobných údajov vrátane metodických usmernení Úradu na ochranu osobných údajov Slovenskej republiky	BL6	11) procesy a metodiky riadenia rizík	BL6	12) postupy analýzy rizík	BL6	13) typické hrozby a postupy pre identifikáciu hrozieb a zraniteľností	BL6	14) bezpečnostné mechanizmy	BL6	15) metodiky podnikovej architektúry	BL6	16) procesy riešenia kybernetických bezpečnostných incidentov	BL6	17) princípy plánovania havarijnej obnovy prevádzky	BL6	18) procesy riadenia kontinuity činností a princípov plánovania havarijnej obnovy	BL6	19) princípy logovania a bezpečnostného monitorovania	BL6	20) zásady riadenia fyzickej a objektovej bezpečnosti	BL6	21) bezpečnostné mechanizmy vo fyzickej a objektovej bezpečnosti	BL6	22) princípy riadenia služieb v oblasti informačných technológií	BL6	23) princípy riadenia nákladov a rozpočtových pravidiel	BL6	24) princípy riadenia ľudských zdrojov	BL6	25) koncepty počítačových sietí	BL6	26) zásady riadenia projektov	BL6
1) procesy a systémy riadenia informačnej a kybernetickej bezpečnosti	BL6																																																				
2) zásady organizácie informačnej a kybernetickej bezpečnosti	BL6																																																				
3) zásady personálnej bezpečnosti	BL6																																																				
4) zásady riadenia prístupov a identít	BL6																																																				
5) spôsob používania kryptografických bezpečnostných mechanizmov	BL6																																																				
6) princípy testovania kybernetickej bezpečnosti	BL6																																																				
7) zásady auditu kybernetickej bezpečnosti	BL6																																																				
8) právne predpisy, požiadavky na súlad a normy vzťahujúce sa na kybernetickú bezpečnosť	BL6																																																				
9) právne predpisy a požiadavky na súlad vzťahujúce sa na ochranu osobných údajov	BL6																																																				
10) štandardy a zásady ochrany osobných údajov vrátane metodických usmernení Úradu na ochranu osobných údajov Slovenskej republiky	BL6																																																				
11) procesy a metodiky riadenia rizík	BL6																																																				
12) postupy analýzy rizík	BL6																																																				
13) typické hrozby a postupy pre identifikáciu hrozieb a zraniteľností	BL6																																																				
14) bezpečnostné mechanizmy	BL6																																																				
15) metodiky podnikovej architektúry	BL6																																																				
16) procesy riešenia kybernetických bezpečnostných incidentov	BL6																																																				
17) princípy plánovania havarijnej obnovy prevádzky	BL6																																																				
18) procesy riadenia kontinuity činností a princípov plánovania havarijnej obnovy	BL6																																																				
19) princípy logovania a bezpečnostného monitorovania	BL6																																																				
20) zásady riadenia fyzickej a objektovej bezpečnosti	BL6																																																				
21) bezpečnostné mechanizmy vo fyzickej a objektovej bezpečnosti	BL6																																																				
22) princípy riadenia služieb v oblasti informačných technológií	BL6																																																				
23) princípy riadenia nákladov a rozpočtových pravidiel	BL6																																																				
24) princípy riadenia ľudských zdrojov	BL6																																																				
25) koncepty počítačových sietí	BL6																																																				
26) zásady riadenia projektov	BL6																																																				

	27) zásady riadenia dodávateľských služieb BL6 28) zásady navrhovania a vývoja aplikácií a informačných systémov BL6 29) zásady obstarávania informačných systémov BL6 30) zásady aplikačnej bezpečnosti BL6 31) princípy a procesy auditovania BL6 32) technické vedomosti o auditovaných systémoch BL6 33) metódy posudzovania rizík dostatočné pre vyhodnotenie rizík auditu a posúdenia hodnotenia rizík, kategorizácie informačných systémov prevádzkovateľov BL6		
Zručnosti:	1) navrhovanie a uplatňovanie bezpečnostných stratégií a politík 2) prioritizácia úloh a efektívne priradovanie zdrojov 3) posudzovanie dôkazov 4) analýza rizík 5) spracovanie úplnej a prehľadnej záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti 6) analýza a hodnotenie bezpečnostných mechanizmov a riešení		
Stupeň vzdelania:	Úplné stredné všeobecné alebo úplné stredné odborné	Vysokoškolské I. stupňa	Vysokoškolské II. a III. stupňa
Odborná prax:	- najmenej 10 rokov praxe v oblasti informačných technológií - z toho najmenej 7 rokov praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT	- najmenej 7 rokov praxe v oblasti informačných technológií - z toho najmenej 5 rokov praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT	- najmenej 5 rokov praxe v oblasti informačných technológií - z toho najmenej 3 roky praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT alebo regulácie kybernetickej bezpečnosti na ústrednom orgáne štátnej správy pre kybernetickú bezpečnosť¹⁾

¹⁾ § 34 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.

Špecifická kvalifikácia:	a) medzinárodný certifikát z oblasti auditu informačných systémov alebo certifikát manažéra kybernetickej bezpečnosti v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti,²⁾ b) zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) schopnosť poskytovať spätnú väzbu d) schopnosť delegovať úlohy e) schopnosť viesť pracovný tím f) schopnosť organizovania a plánovania práce g) analytické myslenie h) tvorivosť (kreativita) i) prezentačná zručnosť

²⁾ Podľa certifikačnej schémy overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti v súlade s STN EN ISO/IEC 17024.

Príloha č. 7
k vyhláške č. 492/2022 Z. z.

Tester kybernetickej bezpečnosti

Rola:	Tester kybernetickej bezpečnosti	
Vedomosti:	Riadenie bezpečnosti 1) zásady organizácie informačnej a kybernetickej bezpečnosti BL3 2) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti BL3 3) princípy riadenia IT služieb, správy systémov a správy počítačových sietí BL3 4) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI, metodiky merania vyspelosti atď.) BL3 5) zdroje, charakteristiky a použitie informačných aktív organizácie BL3 6) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.) BL3 7) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) BL3 8) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly a sieťové služby BL3 9) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.) BL3 10) charakteristiky fyzických a virtuálnych nosičov údajov BL3 11) 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, tlačiarne, vymeniteľné úložné zariadenia, telefóny, faxy atď.) BL3 12) elektrotechnika aplikovaná na architektúru počítačov (napr. základné dosky, procesory, čipy a iný počítačový hardvér) BL3 13) koncepcia a mechanizmy zálohovania a obnovy dát BL3 14) kryptografické algoritmy BL3 15) kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy a steganografia) BL3 16) kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov BL3 17) metódy a politiky správy a štandardizácie údajov BL3	

18) nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti	BL3
19) princípy dolovania a ukladania údajov	BL3
20) princípy elektronickej pošty, vyhľadávacích/analytických techník, nástrojov a používania súborov cookie	BL3
21) princípy webových služieb (napr. architektúra orientovaná na služby, protokol SOAP a jazyk HTML)	BL3
22) princípy zálohovania a obnovy dát	BL3
23) programovacie rozhrania pre prístup k databázam	BL3
24) šifrovacie algoritmy pre lokálne bezdrôtové siete (WLAN)	BL3
25) systémy riadenia bázy dát a ich správa, dopytovacie jazyky, tabuľkové vzťahy	BL3
26) štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch	BL3
27) technológie filtrovania webového obsahu	BL3
28) terminológia dátovej komunikácie (napr. sieťové protokoly, Ethernet, IP, šifrovanie, optické zariadenia, vymeniteľné médiá)	BL3
29) typy sieťovej komunikácie (napr. LAN, WAN, MAN, WLAN, WWAN)	BL3
30) typy webových stránok, správa, funkcie a systémy na správu obsahu (CMS)	BL3
31) XML schémy (Extensible Markup Language)	BL3
32) koncepty kybernetických operácií, terminológia/slovník (t. j. príprava prostredia, kybernetický útok, kybernetická obrana), zásady, obmedzenia a účinky	BL3
33) základy sieťovej a internetovej komunikácie (t. j. zariadenia, konfigurácia zariadení hardvér, softvér, aplikácie, porty, protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.)	BL3
34) princípy zraniteľností bezdrôtových sietí	BL3
Riadenie hrozieb a rizík	
1) procesy riadenia rizík, postupy a metodiky analýzy rizík	BL3
2) typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie	BL3
3) zásady aplikačnej bezpečnosti	BL3
4) teória, koncepty a metódy systémového inžinierstva	BL3
5) metódy a techniky softvérového inžinierstva vrátane modelov vývoja softvéru, princípy životného cyklu vývoja systémov a zásady bezpečného vývoja softvéru	BL3

6) bezpečnostné koncepty v operačných systémoch	BL3
7) bezpečnostné mechanizmy a metódy v softvérovom inžinierstve (napr. modularizácia, vrstvenie, abstrakcia, maskovanie, šifrovanie, pseudonymizácia, minimalizácia spracúvania atď.)	BL3
8) techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť	BL3
9) nástroje na posudzovanie zraniteľností	BL3
10) sieťové protokoly a adresárové služby	BL3
11) architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)	BL3
12) prevádzka webových stránok (napr. webové servery, hosting, DNS, webové jazyky atď.)	BL3
13) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL3*
14) posudzovanie sieťových útokov a vzťahu jednotlivých typov sieťových útokov k hrozbám a zraniteľnostiam	BL3
15) princípy a techniky etického hackingu	BL3
16) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletin)	BL3
17) triedy a vektory útokov	BL3
Aplikácia bezpečnostných opatrení	
1) navrhovanie opatrení na ošetrovanie bezpečnostných rizík	BL3
2) bezpečnostné mechanizmy a spôsob ich implementácie	BL3
3) bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti	BL3
4) nástroje, metódy a techniky navrhovania bezpečnostných systémov	BL3
5) zásady personálnej bezpečnosti	BL3
6) opatrenia týkajúce sa používania, spracovania, uchovávaní a prenosu údajov	BL3
7) zásady a princípy riadenia identít a prístupov	BL3
8) kryptografické bezpečnostné mechanizmy	BL3
9) koncepcie a technológie vzdialeného prístupu	BL3
10) virtualizačné technológie, vývoj a údržba virtuálnych strojov	BL3
11) zabezpečenie virtuálnych privátnych sietí (VPN)	BL3
12) techniky a metódy správy systémov a hardeningu systémov	BL3
Výkon operatívnych bezpečnostných činností	

1) znalosti o štádiách kybernetického útoku (napr. Prieskum, skenovanie, získanie prístupu, eskalácia oprávnení, využitie, zahľadanie stôp)	BL3
2) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia	BL3
3) princípy logovania a bezpečnostného monitorovania	BL3
4) princípy korelácie bezpečnostných udalostí	BL3
5) identifikácia digitálnych stôp a postupy pri ich spracúvaní	BL3
6) princípy, nástroje a techniky testovania prieniku	BL3
7) analýza sieťového prenosu (nástroje, metodiky, procesy)	BL3
8) bezdrôtové technológie (napr. celulárne, satelitné, GSM) zahŕňajúce základnú štruktúru, architektúru a dizajn moderných bezdrôtových komunikačných systémov	BL3
9) charakteristiky komunikačných sietí (napr. kapacita, funkčnosť, trasy, kritické uzly)	BL3
10) forenzné súvislosti štruktúry a procesov operačného systému	BL3
11) koncepcia architektúry sietí vrátane topológie, protokolov, komponentov a bezpečnostných princípov	BL3
12) konfigurácia forenzných laboratórií a podporných aplikácií (napr. VMWare, Wireshark)	BL3
13) mechanizmy zabezpečenia siete (napr. Host based IDS, IPS, ACL) vrátane ich funkcií a umiestnenia v sieti	BL3
14) metódy a nástroje analýzy sieťového prenosu	BL3
15) porty a služby Windows/Unix	BL3
16) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra)	BL3
17) princípy hĺbkovej ochrany a architektúry sieťovej bezpečnosti	BL3
18) princípy sieťových demilitarizovaných zón	BL3
19) princípy súborových systémov (napr. NTFS, FAT a iné)	BL3
20) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii	BL3
21) bezpečnostné zásady správy a údržby databázových systémov	BL3
22) zásady riadenia bezpečnosti prostredia cloudu	BL3
23) základy digitálnej forenznej analýzy pri získavaní použiteľných informácií	BL3
24) zásady riadenia sieťových systémov, modely, metódy (napr. monitorovanie výkonnosti systémov end-to-end)	BL3
25) princípy zraniteľností bezdrôtových sietí	BL3

Zručnosti:	Riadenie bezpečnosti • podpora riadenia informačnej a kybernetickej bezpečnosti organizácie Riadenie hrozieb a rizík a) posudzovanie hrozieb a rizík b) hodnotenie technických zraniteľností systémov c) detekcia, riešenie, evidencia a prevencia kybernetických bezpečnostných incidentov Aplikácia bezpečnostných opatrení a) návrhy zmien a integrácie bezpečnostných technológií a riešení b) podpora riadenia bezpečnostnej architektúry c) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení Výkon operatívnych bezpečnostných činností a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe b) prevádzka technických bezpečnostných opatrení Riadenie súladu a) pravidelné preskúmavanie stavu kybernetickej a informačnej bezpečnosti b) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti
Špecifické kľúčové kompetencie	a) analytické myslenie b) tvorivosť (kreativita)

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

Príloha č. 8
k vyhláške č. 492/2022 Z. z.

Architekt kybernetickej bezpečnosti

Rola:	Architekt 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 BL6 10) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.) BL6 11) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) BL6 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 BL2 15) charakteristiky fyzických a virtuálnych nosičov údajov BL5 16) elektronické zariadenia (napr. počítačové systémy/komponenty, zariadenia na kontrolu prístupu, BL5

	digitálne fotoaparáty, digitálne skenery, pevné disky, pamäťové karty, modemy, sieťové komponenty, sieťové zariadenia, sieťové domáce ovládacie zariadenia, tlačiarne, vymeniteľné úložné zariadenia, telefóny, faxy atď.)	
17)	elektrotechnika aplikovaná na architektúru počítačov (napr. základné dosky, procesory, čipy a iný počítačový hardvér)	BL4
18)	koncepty a mechanizmy zálohovania a obnovy dát	BL6
19)	kryptografické algoritmy	BL5
20)	kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy a steganografia)	BL5
21)	kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov	BL5
22)	metódy a politiky správy a štandardizácie údajov	BL5
23)	nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti	BL6
24)	princípy dolovania a ukladania údajov	BL5
25)	princípy elektronickej pošty, vyhľadávacích/analytických techník, nástrojov a používania súborov cookie	BL6
26)	princípy webových služieb (napr. architektúra orientovaná na služby, protokol SOAP a jazyk HTML)	BL6
27)	princípy zálohovania a obnovy dát	BL6
28)	programovacie rozhrania pre prístup k databázam	BL4
29)	šifrovacie algoritmy pre lokálne bezdrôtové siete (WLAN)	BL5
30)	systémy riadenia bázy dát a ich správa, dopytovacie jazyky, tabuľkové vzťahy	BL4
31)	štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch	BL5
32)	technológie filtrovania webového obsahu	BL5
33)	terminológia dátovej komunikácie (napr. sieťové protokoly, Ethernet, IP, šifrovanie, optické zariadenia, vymeniteľné médiá)	BL6
34)	typy sieťovej komunikácie (napr. LAN, WAN, MAN, WLAN, WWAN)	BL6
35)	typy webových stránok, správa, funkcie a systémy na správu obsahu (CMS)	BL5
36)	XML schémy (Extensible Markup Language)	BL4
37)	koncepty kybernetických operácií, terminológia/slovník (t. j. príprava prostredia, kybernetický útok, kybernetická obrana), zásady, obmedzenia a účinky	BL5
38)	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.)	
39)	princípy zraniteľností bezdrôtových sietí	BL5
	Riadenie hrozieb a rizík	
1)	procesy riadenia rizík, postupy a metodiky analýzy rizík	BL3
2)	typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie	BL6
3)	zásady aplikačnej bezpečnosti	BL6
4)	teória, koncepty a metódy systémového inžinierstva	BL6
5)	metódy a techniky softvérového inžinierstva vrátane modelov vývoja softvéru, princípy životného cyklu vývoja systémov a zásady bezpečného vývoja softvéru	BL6
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.)	BL6
8)	techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť	BL6
9)	nástroje na posudzovanie zraniteľností	BL5
10)	sieťové protokoly a adresárové služby	BL6
11)	architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)	BL6
12)	prevádzka webových stránok (napr. webové servery, hosting, DNS, webové jazyky atď.)	BL6
13)	všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL6*
14)	posudzovanie sieťových útokov a vzťahu jednotlivých typov sieťových útokov k hrozbám a zraniteľnostiam	BL5
15)	princípy a techniky etického hackingu	BL3
16)	princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletin)	BL5
17)	triedy a vektory útokov	BL6
	Aplikácia bezpečnostných opatrení	
1)	navrhovanie opatrení na ošetrenie bezpečnostných rizík	BL6
2)	bezpečnostné mechanizmy a spôsob ich implementácie	BL6
3)	bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti	BL6

4) nástroje, metódy a techniky navrhovania bezpečnostných systémov	BL6
5) zásady personálnej bezpečnosti	BL6
6) opatrenia týkajúce sa používania, spracovania, uchovávaní a prenosu údajov	BL6
7) zásady a princípy riadenia identít a prístupov	BL6
8) kryptografické bezpečnostné mechanizmy	BL6
9) koncepcie a technológie vzdialeného prístupu	BL6
10) virtualizačné technológie, vývoj a údržba virtuálnych strojov	BL6
11) zabezpečenie virtuálnych privátnych sietí (VPN)	BL6
12) techniky a metódy správy systémov a hardeningu systémov	BL6
Výkon operatívnych bezpečnostných činností	
1) znalosti o štádiách kybernetického útoku (napr. prieskum, skenovanie, získanie prístupu, eskalácia oprávnení, využitie, zahľadanie stôp)	BL5
2) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia	BL6
3) princípy logovania a bezpečnostného monitorovania	BL6
4) princípy korelácie bezpečnostných udalostí	BL6
5) bezdrôtové technológie (napr. celulárne, satelitné, GSM) zahŕňajúce základnú štruktúru, architektúru a dizajn moderných bezdrôtových komunikačných systémov	BL5
6) charakteristiky komunikačných sietí (napr. kapacita, funkčnosť, trasy, kritické uzly)	BL2
7) forenzné súvislosti štruktúry a procesov operačného systému	BL2
8) koncepcia architektúry sietí vrátane topológie, protokolov, komponentov a bezpečnostných princípov	BL6
9) mechanizmy zabezpečenia siete (napr. Host based IDS, IPS, ACL) vrátane ich funkcií a umiestnenia v sieti	BL6
10) metódy a nástroje analýzy sieťového prenosu	BL5
11) porty a služby Windows/Unix	BL6
12) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra)	BL6
13) princípy hĺbkovej ochrany a architektúry sieťovej bezpečnosti	BL6
14) princípy súborových systémov (napr. NTFS, FAT a iné)	BL6
15) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii	BL6

	16) bezpečnostné zásady správy a údržby databázových systémov BL5 17) zásady riadenia bezpečnosti prostredia cloudu BL6 18) základy digitálnej forenznej analýzy pri získavaní použiteľných informácií BL4 19) zásady riadenia sieťových systémov, modely, metódy (napr. monitorovanie výkonnosti systémov end-to-end) BL5 20) princípy zraniteľností bezdrôtových sietí BL5 Riadenie súladu 1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť BL5 2) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na ochranu osobných údajov BL5 3) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na prevádzku informačných a komunikačných technológií BL5 4) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky BL5 5) princípy posudzovania kybernetickej bezpečnosti BL5 6) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii BL5 7) štandardy bezpečnosti platobných kariet (PCI) BL6* 8) štandardy a procesy riadenia rizík v dodávateľskom reťazci BL5* 9) metódy testovania a vyhodnocovania bezpečnosti systémov BL5
Zručnosti:	Riadenie bezpečnosti a) podpora riadenia informačnej a kybernetickej bezpečnosti organizácie b) vypracovanie a prezentácia bezpečnostných stratégií a konceptov c) 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 Riadenie hrozieb a rizík a) podpora implementácie procesov a nástrojov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík b) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí c) hodnotenie technických zraniteľností systémov

	Aplikácia bezpečnostných opatrení a) návrhy implementácie, zmien a optimalizácie bezpečnostných technológií a riešení b) podpora riadenia bezpečnostnej architektúry c) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie Výkon operatívnych bezpečnostných činností a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe b) aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov c) riadenie projektov v kybernetickej bezpečnosti Riadenie súladu • budovanie bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov		
Stupeň vzdelania:	Úplné stredné všeobecné alebo úplné stredné odborné	Vysokoškolské I. stupňa	Vysokoškolské II. a III. stupňa
Odborná prax:	• najmenej 3 roky praxe v oblasti informačných technológií	• najmenej 2 roky praxe v oblasti informačných technológií	• najmenej 1 rok praxe v oblasti informačných technológií
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) analytické myslenie d) tvorivosť (kreativita) e) prezentačná zručnosť f) strategické a koncepčné myslenie		

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

Príloha č. 9
k vyhláške č. 492/2022 Z. z.

Špecialista riadenia rizík

Rola:	Špecialista riadenia rizík
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 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) základy Business Continuity Managementu (BCM) BL3 10) poznanie základných procesov pri riadení a obstarávaní informačných systémov vrátane vyhodnocovania dôveryhodnosti dodávateľa alebo výrobku BL3 11) nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti BL4 12) štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch BL5 13) terminológia dátovej komunikácie (napr. sieťové protokoly, Ethernet, IP, šifrovanie, optické zariadenia, vymeniteľné médiá) BL4 14) typy sieťovej komunikácie (napr. LAN, WAN, MAN, WLAN, WWAN) BL4 15) typy webových stránok, správa, funkcie a systémy na správu obsahu (CMS) BL4 16) základy sieťovej a internetovej komunikácie (t. j. zariadenia, konfigurácia zariadení hardvér, softvér, aplikácie, porty/protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.) BL4

17) princípy zraniteľností bezdrôtových sietí	BL4
Riadenie hrozieb a rizík	
1) procesy riadenia rizík, postupy a metodiky analýzy rizík	BL6
2) typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie	BL6
3) zásady aplikačnej bezpečnosti	BL4
4) teória, koncepty a metódy systémového inžinierstva	BL4
5) bezpečnostné koncepty v operačných systémoch	BL3
6) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL4*
7) základné postupy etického hackingu	BL3
8) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletin)	BL5
9) triedy a vektory útokov	BL4
Aplikácia bezpečnostných opatrení	
1) navrhovanie opatrení na ošetrovanie bezpečnostných rizík	BL6
2) bezpečnostné mechanizmy a spôsoby ich implementácie	BL3
3) základné princípy bezpečnostných mechanizmov.	BL3
4) zásady personálnej bezpečnosti	BL5
5) opatrenia týkajúce sa používania, spracovania, uchovávaní a prenosu údajov	BL5
6) zásady a princípy riadenia identít a prístupov	BL4
7) kryptografické bezpečnostné mechanizmy	BL4
8) koncepcie a technológie vzdialeného prístupu	BL4
9) virtualizačné technológie, vývoj a údržba virtuálnych strojov	BL4
Výkon operatívnych bezpečnostných činností	
1) procesy riešenia kybernetických bezpečnostných incidentov	BL4
2) znalosti o štádiách kybernetického útoku (napr. Prieskum, skenovanie, získanie prístupu, eskalácia oprávnení, využitie, zahľadanie stôp)	BL4
3) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia	BL5
4) princípy logovania a bezpečnostného monitorovania	BL4
5) princípy korelácie bezpečnostných udalostí	BL4

	6) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra) BL4 7) princípy hĺbkovej ochrany a architektúry sieťovej bezpečnosti BL3 8) princípy sieťových demilitarizovaných zón BL3 9) princípy súborových systémov (napr. NTFS, FAT a iné) BL3 10) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii BL5 11) zásady riadenia bezpečnosti prostredia cloudu BL3 Riadenie súladu 1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť a ochranu osobných údajov BL6 2) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky BL6 3) princípy posudzovania kybernetickej bezpečnosti BL6 4) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii BL5 5) štandardy bezpečnosti platobných kariet (PCI) BL3* 6) štandardy a procesy riadenia rizík v dodávateľskom reťazci BL6 7) metódy testovania a vyhodnocovania bezpečnosti systémov BL3
Zručnosti:	Riadenie bezpečnosti podpora riadenia informačnej a kybernetickej bezpečnosti organizácie Riadenie hrozieb a rizík a) implementácia procesov a nástrojov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík b) posudzovanie hrozieb a rizík c) návrh opatrení na ošetrovanie rizík d) účasť v procesoch obnovy prevádzkových činnosti (tzv. Business Continuity Management) vrátane účasti v riadení procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning) Aplikácia bezpečnostných opatrení a) podpora riadenia bezpečnostnej architektúry

	b) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení Výkon operatívnych bezpečnostných činností a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe b) aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov Riadenie súladu a) pravidelné preskúmavanie stavu kybernetickej a informačnej bezpečnosti b) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) analytické myslenie d) prezentačná zručnosť e) schopnosť organizovania a plánovania práce f) strategické a koncepčné myslenie

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

Príloha č. 10
k vyhláške č. 492/2022 Z. z.

Špecialista pre analýzu digitálnych stôp

Rola:	Špecialista pre analýzu digitálnych stôp
Vedomosti:	Riadenie bezpečnosti 1) zásady organizácie informačnej a kybernetickej bezpečnosti BL4 2) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti BL4 3) princípy riadenia IT služieb, správy systémov a správy počítačových sietí BL4 4) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI, metodiky merania vyspelosti atď.) BL5 5) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) BL6 6) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly a sieťové služby BL6 7) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.) BL6 8) charakteristiky fyzických a virtuálnych nosičov údajov BL6 9) 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, tlačiarne, vymeniteľné úložné zariadenia, telefóny, faxy atď.) BL6 10) elektrotechnika aplikovaná na architektúru počítačov (napr. základné dosky, procesory, čipy a iný počítačový hardvér) BL6 11) koncepcia a mechanizmy zálohovania a obnovy dát BL6 12) kryptografické algoritmy BL5 13) kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy a steganografia) BL5 14) kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov BL5 15) metódy a politiky správy a štandardizácie údajov BL6 16) nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti BL6 17) princípy dolovania a ukladania údajov BL6 18) princípy elektronickej pošty, vyhľadávacích/analytických technik, nástrojov a používania súborov cookie BL6 19) princípy webových služieb (napr. architektúra orientovaná na služby, protokol SOAP a jazyk HTML) BL6

20) princípy zálohovania a obnovy dát	BL6
21) programovacie rozhrania pre prístup k databázam	BL5
22) šifrovacie algoritmy pre lokálne bezdrôtové siete (WLAN)	BL5
23) systémy riadenia bázy dát a ich správa, dopytovacie jazyky, tabuľkové vzťahy	BL5
24) štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch	BL5
25) technológie filtrovania webového obsahu	BL5
26) terminológia dátovej komunikácie (napr. sieťové protokoly, Ethernet, IP, šifrovanie, optické zariadenia, vymeniteľné médiá)	BL6
27) typy sieťovej komunikácie (napr. LAN, WAN, MAN, WLAN, WWAN)	BL6
28) typy webových stránok, správa, funkcie a systémy na správu obsahu (CMS)	BL5
29) XML schémy (Extensible Markup Language)	BL5
30) koncepty kybernetických operácií, terminológia/slovník (t. j. príprava prostredia, kybernetický útok, kybernetická obrana), zásady, obmedzenia a účinky	BL6
31) základy sieťovej a internetovej komunikácie (t. j. zariadenia, konfigurácia zariadení hardvér, softvér, aplikácie, porty/protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.)	BL6
32) princípy zraniteľností bezdrôtových sietí	BL6
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	BL5
4) teória, koncepty a metódy systémového inžinierstva	BL5
5) bezpečnostné koncepty v operačných systémoch	BL5
6) bezpečnostné mechanizmy a metódy v softvérovom inžinierstve (napr. modularizácia, vrstvenie, abstrakcia, maskovanie, šifrovanie, pseudonymizácia, minimalizácia spracúvania atď.)	BL5
7) techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť	BL6
8) nástroje na posudzovanie zraniteľností	BL6
9) sieťové protokoly a adresárové služby	BL6
10) architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)	BL6

11) prevádzka webových stránok (napr. webové servery, hosting, DNS, webové jazyky atď.)	BL6
12) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL5*
13) posudzovanie sieťových útokov a vzťahu jednotlivých typov sieťových útokov k hrozbám a zraniteľnostiam	BL6
14) princípy a techniky etického hackingu	BL5
15) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletin)	BL6
16) triedy a vektory útokov	BL6
Aplikácia bezpečnostných opatrení	
1) bezpečnostné mechanizmy a spôsob ich implementácie	BL6
2) opatrenia týkajúce sa používania, spracovania, uchovávaní a prenosu údajov	BL6
3) zásady a princípy riadenia identít a prístupov	BL6
4) koncepcie a technológie vzdialeného prístupu	BL6
5) virtualizačné technológie, vývoj a údržba virtuálnych strojov	BL6
6) zabezpečenie virtuálnych privátnych sietí (VPN)	BL6
7) techniky a metódy správy systémov a hardeningu systémov	BL6
Výkon operatívnych bezpečnostných činností	
1) procesy riešenia kybernetických bezpečnostných incidentov	BL6
2) znalosti o štádiách kybernetického útoku (napr. Prieskum, skenovanie, získanie prístupu, eskalácia oprávnení, využitie, zahľadanie stôp)	BL6
3) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia	BL6
4) princípy logovania a bezpečnostného monitorovania	BL6
5) princípy korelácie bezpečnostných udalostí	BL6
6) identifikácia digitálnych stôp a postupy pri ich spracúvaní	BL6
7) princípy, nástroje a techniky testovania prieniku	BL6
8) analýza sieťového prenosu (nástroje, metodiky, procesy)	BL6
9) bezdrôtové technológie (napr. celulárne, satelitné, GSM) zahŕňajúce základnú štruktúru, architektúru a dizajn moderných bezdrôtových komunikačných systémov	BL5
10) charakteristiky komunikačných sietí (napr. kapacita, funkčnosť, trasy, kritické uzly)	BL6

11) forenzné súvislosti štruktúry a procesov operačného systému	BL6
12) koncepcia architektúry sietí vrátane topológie, protokolov, komponentov a bezpečnostných princípov	BL6
13) konfigurácia forenzných laboratórií a podporných aplikácií (napr. VMWare, Wireshark)	BL6
14) mechanizmy zabezpečenia siete (napr. Host based IDS, IPS, ACL) vrátane ich funkcií a umiestnenia v sieti	BL6
15) metódy a nástroje analýzy sieťového prenosu	BL6
16) porty a služby Windows/Unix	BL6
17) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra)	BL6
18) princípy hĺbkovej ochrany a architektúry sieťovej bezpečnosti	BL6
19) princípy sieťových demilitarizovaných zón	BL6
20) princípy súborových systémov (napr. NTFS, FAT a iné)	BL6
21) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii	BL6
22) bezpečnostné zásady správy a údržby databázových systémov	BL6
23) zásady riadenia bezpečnosti prostredia cloudu	BL6
24) základy digitálnej forenznej analýzy pri získavaní použiteľných informácií	BL6
25) 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	BL5
6) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii	BL4
7) štandardy bezpečnosti platobných kariet (PCI)	BL5*
8) metódy testovania a vyhodnocovania bezpečnosti systémov	BL5

Zručnosti:	Riadenie bezpečnosti • podpora riadenia informačnej a kybernetickej bezpečnosti organizácie Riadenie hrozieb a rizík a) posudzovanie hrozieb a rizík b) hodnotenie technických zraniteľností systémov c) detekcia, riešenie, evidencia a prevencia kybernetických bezpečnostných incidentov Aplikácia bezpečnostných opatrení • predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie Výkon operatívnych bezpečnostných činností • výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe Riadenie súladu a) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti b) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní
Špecifické kľúčové kompetencie	a) schopnosť myslieť a konať v súvislostiach b) analytické myslenie c) tvorivosť (kreativita) d) prezentačná zručnosť

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

Príloha č. 11
k vyhláške č. 492/2022 Z. z.

Špecialista pre riadenie súladu

Rola:	Špecialista pre riadenie súladu
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 BL4 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 BL4 10) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) BL3 11) kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy a steganografia) BL3 12) kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov BL3 13) nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti BL3 14) princípy zálohovania a obnovy dát BL6 15) štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch 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 BL3

3) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL3*
4) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletin)	BL3
5) triedy a vektory útokov	BL3
Aplikácia bezpečnostných opatrení	
1) navrhovanie opatrení na ošetrovanie bezpečnostných rizík	BL3
2) bezpečnostné mechanizmy a spôsob ich implementácie	BL3
3) bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti	BL3
4) zásady personálnej bezpečnosti	BL3
5) opatrenia týkajúce sa používania, spracovania, uchovávaní a prenosu údajov	BL3
6) zásady a princípy riadenia identít a prístupov	BL3
7) kryptografické bezpečnostné mechanizmy	BL3
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, zahľadanie stôp)	BL4
3) princípy logovania a bezpečnostného monitorovania	BL3
4) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra)	BL3
5) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii	BL5
6) zásady riadenia bezpečnosti prostredia cloudu	BL3
Riadenie súladu	
1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť	BL6
2) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na ochranu osobných údajov	BL6
3) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na prevádzku informačných a komunikačných technológií	BL6
4) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky	BL6
5) princípy posudzovania kybernetickej bezpečnosti	BL4

	6) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii BL6 7) zásady a metódy tvorby učebných plánov, výuky jednotlivcov a skupín BL5 8) štandardy bezpečnosti platobných kariet (PCI) BL6* 9) štandardy a procesy riadenia rizík v dodávateľskom reťazci BL5
Zručnosti:	Riadenie bezpečnosti a) podpora riadenia informačnej a kybernetickej bezpečnosti organizácie b) vypracovanie a prezentácia bezpečnostných stratégií a konceptov c) implementácia procesov informačnej a kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov d) zabezpečenie, vypracovanie, udržiavanie a aktualizácie bezpečnostnej dokumentácie informačnej a kybernetickej bezpečnosti a ďalších interných riadiacich aktov vo vzťahu k bezpečnosti organizácie e) 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 f) riadenie informačnej a kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri zaobstarávaní, projektovaní a vývoji softvéru a systémov g) správa bezpečnosti informačných aktív organizácie Riadenie hrozieb a rizík a) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí b) evidencia a prevencia kybernetických bezpečnostných incidentov Aplikácia bezpečnostných opatrení a) návrhy zmien a integrácie bezpečnostných technológií a riešení b) podpora riadenia bezpečnostnej architektúry c) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie Výkon operatívnych bezpečnostných činností

	a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe b) aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov c) zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov Riadenie súladu a) pravidelné preskúmavanie stavu kybernetickej a informačnej bezpečnosti b) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti c) budovanie bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov d) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) analytické myslenie d) prezentačná zručnosť e) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí f) schopnosť organizovania a plánovania práce g) strategické a koncepčné myslenie

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

Príloha č. 12
k vyhláške č. 492/2022 Z. z.

Špecialista pre riešenie kybernetických incidentov

Rola:	Špecialista pre riešenie kybernetických incidentov
Vedomosti:	Riadenie bezpečnosti 1) procesy, systémy a zásady riadenia informačnej a kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti BL2 2) zásady organizácie informačnej a kybernetickej bezpečnosti BL2 3) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti BL6 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 BL6 7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami BL6 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.) BL4 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.) BL6 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) elektronické zariadenia (napr. počítačové systémy/komponenty, zariadenia na kontrolu prístupu, BL6

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

	aplikácie, porty/protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.)	
39)	princípy zraniteľností bezdrôtových sietí	BL6
	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	BL6
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	BL4
6)	bezpečnostné koncepty v operačných systémoch	BL6
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	BL6
9)	nástroje na posudzovanie zraniteľností	BL6
10)	sieťové protokoly a adresárové služby	BL6
11)	architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)	BL6
12)	prevádzka webových stránok (napr. webové servery, hosting, DNS, webové jazyky atď.)	BL6
13)	všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL6*
14)	posudzovanie sieťových útokov a vzťahu jednotlivých typov sieťových útokov k hrozbám a zraniteľnostiam	BL6
15)	princípy a techniky etického hackingu	BL6
16)	princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletin)	BL6
17)	triedy a vektory útokov	BL6
	Aplikácia bezpečnostných opatrení	
1)	navrhovanie opatrení na ošetrenie bezpečnostných rizík	BL6
2)	bezpečnostné mechanizmy a spôsob ich implementácie	BL6
3)	bezpečnostné opatrenia vo fyzickej a objektivej bezpečnosti	BL6

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

	17) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra)	BL6
	18) princípy hlbkovej ochrany a architektúry sieťovej bezpečnosti	BL6
	19) princípy sieťových demilitarizovaných zón	BL6
	20) princípy súborových systémov (napr. NTFS, FAT a iné)	BL6
	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	BL6
	24) základy digitálnej forenznej analýzy pri získavaní použiteľných informácií	BL6
	25) zásady riadenia sieťových systémov, modely, metódy (napr. monitorovanie výkonnosti systémov end-to-end)	BL5
	26) princípy zraniteľností bezdrôtových sietí	BL6
	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	BL5
	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:	Riadenie bezpečnosti	
	a) podpora riadenia informačnej a kybernetickej bezpečnosti organizácie	
	b) správa bezpečnosti informačných aktív organizácie	

	Riadenie hrozieb a rizík a) implementácia procesov a nástrojov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík b) posudzovanie hrozieb a rizík c) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí d) hodnotenie technických zraniteľností systémov e) detekcia, riešenie, evidencia a prevencia kybernetických bezpečnostných incidentov f) koordinácia procesov obnovy prevádzkových činností (tzv. Business Continuity Management) vrátane riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning) Aplikácia bezpečnostných opatrení a) zabezpečovanie implementácie technických a organizačných bezpečnostných opatrení b) návrhy zmien a integrácie bezpečnostných technológií a riešení c) podpora riadenia bezpečnostnej architektúry Výkon operatívnych bezpečnostných činností a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe b) prevádzka technických bezpečnostných opatrení Riadenie súladu a) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti b) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) analytické myslenie d) tvorivosť (kreativita) e) schopnosť organizovania a plánovania práce

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

Príloha č. 13
k vyhláške č. 492/2022 Z. z.

Analytik kybernetickej bezpečnosti

Rola:	Analytik kybernetickej bezpečnosti	
Vedomosti:	Riadenie bezpečnosti	
	1) procesy, systémy a zásady riadenia informačnej a kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti	BL5
	2) organizácia informačnej a kybernetickej bezpečnosti	BL6
	3) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti	BL6
	4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí	BL5
	5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI atď.)	BL5
	6) zdroje, charakteristiky a použitie informačných aktív organizácie	BL6
	7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami	BL6
	8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI)	BL6
	9) zásady a techniky plánovania kapacity a plánovania zdrojov	BL5
	10) princípy riadenia ľudských zdrojov	BL6
	11) rozpočtové pravidlá, zásady plánovania a riadenia nákladov a plánovania a riadenia investícií	BL5
	12) procesy riadenia kontinuity činností a plánovania havarijnej obnovy prevádzky	BL6
	13) výskumné stratégie a znalostný manažment	BL4
	14) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.)	BL5
	15) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.)	BL4
	16) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly	BL5
	17) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.)	BL4
	18) zásady riadenia dodávateľských služieb a obstarávania informačných systémov vrátane vyhodnocovania dôveryhodnosti dodávateľa alebo výrobku	BL6

Riadenie hrozieb a rizík		
1) procesy riadenia rizík, postupy a metodiky analýzy rizík		BL6
2) typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie		BL5
3) zásady aplikačnej bezpečnosti		BL5
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.)		BL5
8) techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť		BL4
9) nástroje na posudzovanie zraniteľností		BL3
10) sieťové protokoly a adresárové služby		BL3
11) základná architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)		BL3
12) bezpečnostné riziká cloud computingu		BL4
13) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)		BL5*
Aplikácia bezpečnostných opatrení		
1) princípy navrhovania opatrení na ošetrovanie bezpečnostných rizík		BL6
2) bezpečnostné mechanizmy a spôsob ich implementácie		BL5
3) bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti		BL5
4) nástroje, metódy a techniky navrhovania bezpečnostných systémov		BL4
5) zásady personálnej bezpečnosti		BL5
6) opatrenia týkajúce sa používania, spracovania, uchovávaní a prenosu údajov		BL6
7) zásady a princípy riadenia identít a prístupov		BL5
8) základy kryptografických bezpečnostných mechanizmov		BL4
9) koncepcie a technológie vzdialeného prístupu		BL4
10) virtualizačné technológie, vývoja a údržby virtuálnych strojov		BL4

	11) zabezpečenie virtuálnych privátnych sietí (VPN) 12) techniky a metódy správy systémov a hardeningu systémov Výkon operatívnych bezpečnostných činností 1) procesy riešenia kybernetických bezpečnostných incidentov 2) zásady riadenia bezpečnosti prostredia cloudu 3) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia 4) princípy logovania a bezpečnostného monitorovania 5) princípy korelácie bezpečnostných udalostí 6) základné postupy pri spracovaní digitálnych stôp 7) princípy, nástroje a techniky testovania prieniku Riadenie súladu 1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť a ochranu osobných údajov 2) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na prevádzku informačných a komunikačných technológií 3) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky 4) princípy posudzovania kybernetickej bezpečnosti 5) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii 6) systémy odbornej prípravy, princípy vzdelávacích stratégií, procesov a postupov vzdelávania a zvyšovania povedomia u dospelých v oblasti kybernetickej bezpečnosti vrátane merania efektivity vzdelávania 7) zásady a metódy tvorby učebných plánov, výuky jednotlivcov a skupín 8) štandardy bezpečnosti platobných kariet (PCI) 9) štandardy a procesy riadenia rizík v dodávateľskom reťazci 10) metódy testovania a vyhodnocovania bezpečnosti systémov	BL4 BL4 BL6 BL5 BL4 BL4 BL4 BL4 BL4 BL6 BL6 BL6 BL5 BL6 BL6 BL6 BL5* BL6 BL6
Zručnosti:	Riadenie bezpečnosti a) strategické riadenie informačnej a kybernetickej bezpečnosti organizácie b) vypracovanie a prezentácia bezpečnostných stratégií a konceptov	

	c) implementácia a riadenie procesov informačnej a kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov d) zabezpečenie, vypracovanie, udržiavanie a aktualizácie bezpečnostnej dokumentácie informačnej a kybernetickej bezpečnosti a ďalších interných riadiacich aktov vo vzťahu k bezpečnosti organizácie e) návrh požiadaviek na rozpočet a na iné zdroje súvisiace s bezpečnostnými opatreniami a procesmi relevantnými z hľadiska informačnej a kybernetickej bezpečnosti vrátane riadenia nákladov a riadenia investícií f) 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 g) poskytovanie informácií bezpečnostnému výboru alebo štatutárnemu orgánu o stave informačnej a kybernetickej bezpečnosti v organizácii, o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach h) riadenie informačnej a kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri obstarávaní a vývoji softvéru a systémov Riadenie hrozieb a rizík a) implementácia a manažment procesov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík b) posudzovanie hrozieb a rizík c) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí d) zabezpečovanie procesov hodnotenia technických zraniteľností systémov e) manažment procesov detekcie, riešenia, evidencie a prevencie kybernetických bezpečnostných incidentov f) zabezpečenie funkčných plánov continuity a obnovy činností organizácie g) koordinácia a riadenie procesov obnovy prevádzkových činností (tzv. Business Continuity Management) vrátane riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning) Aplikácia bezpečnostných opatrení a) riadenie návrhov, implementácie, zmien a optimalizácie bezpečnostných riešení s víziou a konceptom ich bežného prevádzkovania
--	--

	b) zabezpečovanie implementácie technických a organizačných bezpečnostných opatrení c) riadenie návrhov, zmien a integrácie bezpečnostných technológií a riešení d) riadenie bezpečnostnej architektúry e) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie f) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení Výkon operatívnych bezpečnostných činností a) manažment výkonu činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe b) vedenie tímu zamestnancov útvaru informačnej a kybernetickej bezpečnosti, ak je taký organizačný útvar zriadený c) návrh a aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov d) riadenie bežnej prevádzky technických bezpečnostných opatrení e) zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov f) zaistenie uplatňovania princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie g) riadenie projektov kybernetickej bezpečnosti Riadenie súladu a) riadenie procesov zaručenia súladu (tzv. Compliance Management) v oblasti informačnej a kybernetickej bezpečnosti b) zabezpečenie pravidelného preskúmavania stavu kybernetickej a informačnej bezpečnosti c) vyhodnocovanie plnenia vnútorných predpisov súvisiacich s riadením kybernetickej bezpečnosti d) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti e) navrhovanie metrik a kľúčových indikátorov pre sledovanie vývoja a stavu bezpečnosti a vývoja bezpečnostných rizík f) zabezpečovanie školení zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti g) zabezpečovanie kontinuálneho vzdelávania pre pracovné roly relevantné z hľadiska kybernetickej bezpečnosti h) zabezpečovanie budovania bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov
--	---

	i) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní		
Stupeň vzdelania:	Úplné stredné všeobecné alebo úplné stredné odborné	Vysokoškolské I. stupňa	Vysokoškolské II. a III. stupňa
Odborná prax:	- najmenej 7 rokov praxe v oblasti informačných technológií - z toho najmenej 5 rokov praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok	- najmenej 5 rokov praxe v oblasti informačných technológií - z toho najmenej 3 roky praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok	- 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 - medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) schopnosť riešiť konflikty d) schopnosť poskytovať spätnú väzbu e) schopnosť delegovať úlohy f) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí g) schopnosť viesť pracovný tím h) schopnosť organizovania a plánovania práce i) analytické myslenie j) strategické a koncepčné myslenie k) tvorivosť (kreativita) l) prezentačná zručnosť		

Príloha č. 14
k vyhláške č. 492/2022 Z. z.

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, bulletin)	BL5
17) triedy a vektory útokov	BL5
Aplikácia bezpečnostných opatrení	
1) navrhovanie opatrení na ošetrovanie 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, uchovávaní 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, zahľadenie 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 forenzej 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 úrovni 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

