Pracovník/pracovnice bezpečnostního dohledového centra informačních systémů (kód: 18-020-M)

Autorizující orgán: Národní úřad pro kybernetickou a informační bezpečnost
Skupina oborů: Informatické obory (kód: 18)
Týká se povolání: Pracovník bezpečnostního dohledového centra informačních systémů
Kvalifikační úroveň NSK - EQF: 4

Odborná způsobilost

Název	Úroveň
Orientace ve webových technologiích	4
Aplikace právních základů kybernetické bezpečnosti při analýze incidentů	5
Sběr dat a analýza údajů v oblasti kybernetické bezpečnosti	5
Organizace činností směřujících k zajištění a obnovení kybernetické bezpečnosti	4
Základní instalace operačního systému a jeho konfigurace	3
Konfigurace síťových připojení	4
Zabezpečení dat před zneužitím	4
Ochrana dat před zničením, zálohování dat	4
Správa počítačových sítí z hlediska jejich funkčnosti a bezpečnosti	4
Organizace činností směřujících k poskytování informací o kybernetických hrozbách a jejich prevenci	4
Základní identifikace a popis kybernetických hrozeb a typů útoků	4
Monitorování provozu počítačových sítí pro potřeby pracovníka/pracovnice bezpečnostního dohledového centra	4
Základy monitorování provozu operačních systémů, jejich diagnostika a optimalizace výkonu	3
Vedení a udržování dokumentace struktury počítačových sítí a operačních systémů	4

Platnost standardu

Standard je platný od: 20.05.2025

Kritéria a způsoby hodnocení

Orientace ve webových technologiích

Kritéria hodnocení	Způsoby ověření
a) Orientovat se v základních webových technologiích a jejich použití	Ústní ověření
b) Vysvětlit termíny/pojmy spojené s webovými technologiemi: databáze, server, klient, apache, IIS, MySQL, WAF, NGINX, OWASP	Ústní ověření

Je třeba splnit obě kritéria.

Aplikace právních základů kybernetické bezpečnosti při analýze incidentů

Kritéria hodnocení	Způsoby ověření
a) Orientovat se v obsahu jednotlivých částí zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, které jsou zaměřeny na analýzu incidentů	Ústní ověření
b) Vysvětlit části prováděcích předpisů vztahujících se k zákonu č. 181/2014 Sb. (vyhláška č. 82/2018 Sb. a nařízení vlády č. 432/2010 včetně jeho pozdějších příloh a změn), které jsou zaměřeny na analýzu incidentů	Ústní ověření
c) Vyplnit hlášení kybernetického bezpečnostního incidentu	Praktické předvedení

Je třeba splnit všechna kritéria.

Sběr dat a analýza údajů v oblasti kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Definovat metody sběru dat v kybernetické bezpečnosti a jejich zpracování	Ústní ověření
b) Provést analýzu údajů a sběru dat pro kybernetickou bezpečnost	Praktické předvedení a ústní ověření
c) Vysvětlit postup při zpracování zpráv a výkazů pro dohledové centrum, požadavky rozlišení adresátů v souladu se zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy	Ústní ověření
d) Charakterizovat základní pojmy a procesy CSIRT týmů (ve smyslu RFC 2350)	Ústní ověření
e) Vysvětlit pojem threat hunting s uvedením příkladů nad různými druhy dat	Ústní ověření
f) Popsat a vysvětlit hlavní funkce SIEM	Ústní ověření
g) Prezentovat metody sběru dat v kybernetické bezpečnosti a jejich zpracování	Praktické předvedení a ústní ověření

Je třeba splnit všechna kritéria.

Organizace činností směřujících k zajištění a obnovení kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Popsat koordinaci činností směřujících k zajištění a obnovení kybernetické bezpečnosti s příslušnou autoritou (NCKB, CZ.NIC)	Ústní ověření
b) Definovat a vysvětlit pravidla a povinnosti při zjištění kybernetického bezpečnostního incidentu (KBI) a zajištění důkazů	Ústní ověření

Je třeba splnit obě kritéria.

Základní instalace operačního systému a jeho konfigurace

Kritéria hodnocení	Způsoby ověření
a) Nainstalovat operační systém ze skupiny Windows	Praktické předvedení
b) Nainstalovat operační systém ze skupiny Linux/FreeBSD	Praktické předvedení
c) Správně nakonfigurovat firewall na jednom z nainstalovaných operačních systémů	Praktické předvedení

Je třeba splnit všechna kritéria.

Konfigurace síťových připojení

Kritéria hodnocení	Způsoby ověření
a) Charakterizovat základní parametry (IP adresa, maska, výchozí brána, DNS, MAC adresa) pro konfiguraci síťového připojení	Ústní ověření
b) Vysvětlit postup konfigurace síťového připojení v různých operačních systémech	Ústní ověření
c) Správně nastavit síťové připojení počítače	Praktické předvedení a ústní ověření
d) Navrhnout způsob zabezpečení bezdrátové sítě (WPA-Enterprise/radius, WIDS/WIPS)	Praktické předvedení a ústní ověření

Je třeba splnit všechna kritéria.

Zabezpečení dat před zneužitím

Kritéria hodnocení	Způsoby ověření
a) Analyzovat stav a bezpečnostní rizika s ohledem na konkrétní řešení	Praktické předvedení
b) Navrhnout řešení zabezpečení dat před zneužitím (např. šifrování disků, triáda CIA, použití PKI)	Praktické předvedení a ústní ověření
c) Provést analýzu PCAP souboru ve Wiresharku (demonstrovat navázaní TCP handshake, DHCP broadcast, nalezení plaintext password v FTP přenosu apod.)	Praktické předvedení a ústní ověření
d) Popsat principy bezpečného chování uživatele na internetu	Ústní ověření
e) Vysvětlit princip firewallu	Ústní ověření
f) Prokázat znalost terminologie, funkcí a parametrů prostředků z oblasti zabezpečení dat	Písemné ověření
g) Popsat principy kryptografie	Ústní ověření
h) Vysvětlit pojmy symetrický/asymetrický klíč, hashovací funkce, elektronický podpis, časové razítko	Ústní ověření

Je třeba splnit všechna kritéria.

Ochrana dat před zničením, zálohování dat

Kritéria hodnocení	Způsoby ověření
a) Navrhnout řešení zálohování dat (např. zvolit zálohovací médium, software, navrhnout plán záloh, vysvětlit rizika)	Praktické předvedení a ústní ověření
b) Zálohovat a obnovit data pomocí vhodného nástroje	Praktické předvedení
c) Prokázat znalost terminologie, funkcí a parametrů prostředků z oblasti ochrany dat (např. plná záloha, přírůstková záloha, zálohovací média a zařízení)	Písemné ověření

Je třeba splnit všechna kritéria.

Správa počítačových sítí z hlediska jejich funkčnosti a bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Charakterizovat základní pravidla a postupy při zabezpečení počítačových sítí	Ústní ověření
b) Popsat a definovat základní prvky počítačových sítí a jejich funkcionality	Ústní ověření

Je třeba splnit obě kritéria.

Organizace činností směřujících k poskytování informací o kybernetických hrozbách a jejich prevenci

Kritéria hodnocení	Způsoby ověření
a) Popsat pravidla psaní zpráv o kybernetických hrozbách a doporučení v kybernetické bezpečnosti	Ústní ověření
b) Popsat pravidla a postup publikace preventivních a metodických informací a pravidla spolupráce v oblasti publikování v kybernetické bezpečnosti. Specifikovat úlohu GOVCERT týmu a Národního CERT/CSIRT týmu	Ústní ověření

Je třeba splnit obě kritéria.

Základní identifikace a popis kybernetických hrozeb a typů útoků

Kritéria hodnocení	Způsoby ověření
a) Definovat a analyzovat základní typy kybernetických útoků a vysvětlit jejich princip	Praktické předvedení a ústní ověření
b) Vysvětlit termíny a pojmy malware, phishing a sociální inženýrství, CVE, MITRE ATT&CK ve spojení s kybernetickými útoky	Ústní ověření

Je třeba splnit obě kritéria.

Monitorování provozu počítačových sítí pro potřeby pracovníka/pracovnice bezpečnostního dohledového centra

Kritéria hodnocení	Způsoby ověření
a) Popsat referenční model ISO/OSI včetně jeho 7 vrstev	Ústní ověření
b) Popsat nástroje používané pro provozní monitoring počítačových sítí	Ústní ověření
c) Vysvětlit pojmy TTL, jitter, zpoždění při přenosu a popsat základní rozdíl mezi TCP a UDP protokolem	Ústní ověření
d) Popsat účel segmentace sítí	Ústní ověření
e) Popsat protokoly aplikační vrstvy (HTTP, POP3, IMAP, SMTP, DNS)	Ústní ověření
f) Na příkladu demonstrovat rozdíl mezi protokolem telnet a ssh na zachycených síťových provozech	Praktické předvedení a ústní ověření

Je třeba splnit všechna kritéria.

Základy monitorování provozu operačních systémů, jejich diagnostika a optimalizace výkonu

Kritéria hodnocení	Způsoby ověření
a) Specifikovat základní parametry, které je vhodné monitorovat v rámci monitoringu provozu operačních systémů	Ústní ověření
b) Definovat základní nástroje pro diagnostiku a monitoring hardware a software a vysvětlit, k čemu tyto nástroje slouží	Ústní ověření
c) Provést základní diagnostiku operačního systému a optimalizaci výkonu dle zadání	Praktické předvedení a ústní ověření

Je třeba splnit všechna kritéria.

Vedení a udržování dokumentace struktury počítačových sítí a operačních systémů

Kritéria hodnocení	Způsoby ověření
a) Vysvětlit důvody pro udržování aktuální dokumentace počítačových sítí a operačních systémů a dopady, které může mít její absence	Ústní ověření
b) Definovat a popsat nástroje pro tvorbu dokumentace počítačové sítě a operačního systému	Ústní ověření

Je třeba splnit obě kritéria.

Organizační a metodické pokyny

Pokyny k realizaci zkoušky

1. Vstupní předpoklady pro účast na zkoušce

Uchazečem o zkoušku může být každá fyzická osoba starší 18 let, která získala alespoň základy vzdělání, nebo účastník rekvalifikace podle zákona č. 435/2004 Sb., zákon o zaměstnanosti.

Zdravotní způsobilost není vyžadována.

Autorizovaná osoba zároveň s odesláním pozvánky ke zkoušce písemnou formou sdělí, kde a jakým způsobem se uchazeč může informovat o svých povinnostech a průběhu zkoušky a které doklady/dokumenty musí uchazeč předložit bezprostředně před započetím zkoušky.

Autorizovaná osoba informuje žadatele písemnou formou v předstihu minimálně 7 dní o vybraných technologiích (HW a SW) a platformách zvolených pro vykonání zkoušky.

2. Průběh zkoušky

Před zahájením zkoušky uchazeč předloží zkoušejícímu průkaz totožnosti a případně další dokumenty opravňující k připuštění ke zkoušce uvedené v části 1. Vstupní předpoklady pro účast na zkoušce.

Bezprostředně před zahájením zkoušky autorizovaná osoba seznámí uchazeče s pracovištěm, s organizací zkoušky, s jeho právy a povinnostmi v rámci zkoušky dle zákona č. 179/2006 Sb. a s požadavky bezpečnosti a ochrany zdraví při práci (BOZP) a požární ochrany (PO), o čemž bude autorizovanou osobou vyhotoven a uchazečem podepsán písemný záznam.

Zkoušející uzná, a tedy nemusí ověřovat, ty odborné způsobilosti, které byly již dříve u uchazeče ověřeny v rámci zkoušky z jiné profesní kvalifikace (nutno doložit osvědčením o získání profesní kvalifikace), a které jsou shodné svým rozsahem i obsahem. Rozsah a obsah odborné způsobilosti určují její jednotlivá kritéria a pokyny k realizaci zkoušky popsané v hodnoticím standardu. Zkoušející tyto odborné způsobilosti neuzná jako již ověřené, pokud by tím nebylo zajištěno řádné ověření ostatních požadavků stanovených tímto hodnoticím standardem (například při nutnosti dodržení technologických postupů a časové souslednosti různých činností).

Zkouška se koná v českém jazyce.

Zkouška je veřejná. Praktická část zkoušky a praktická zkouška není veřejná v případech, kdy to je nutné z hygienických důvodů nebo z důvodu ochrany zdraví a bezpečnosti práce.

Pokyny k jednotlivým způsobům ověřování:

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „***písemné ověření***":

Uchazeč v první části zkoušky prokáže znalosti písemným testem (délka 15 min., rozsah 10 otázek).
Pravidla pro aplikaci testů:
Soubor otázek pro testy stanovuje autorizovaná osoba podle požadavků hodnoticího standardu.
Musí přitom splňovat následující pravidla:

- Testy pro jednotlivé uchazeče musí být vygenerovány z dostatečně velkého souboru otázek, aby bylo možné vytvářet dostatečné počty různě sestavených testů.
- Při každé zkoušce musí být ověřeny všechny odborné způsobilosti.
- Každý uchazeč má ve svém testu pro každé kritérium, u kterého je uveden písemný způsob ověření, alespoň jednu otázku.

Za úspěšné splnění testu se považuje 70 % správně zodpovězených otázek s tím, že pro každé kritérium musí být správně zodpovězeno alespoň 50 % otázek.

Autorizovaná osoba vypracuje soubor 30 testových otázek, zaměřených na ověření znalostní složky vybraných odborných způsobilostí:

- *Zabezpečení dat před zneužitím*, kritérium f) 15 otázek
- *Ochrana dat před zničením, zálohování dat*, kritérium c) 15 otázek

Autorizovaná osoba zajistí vygenerování náhodného testu pro každého uchazeče, sestaveného z 10 otázek s následujícím zastoupením jednotlivých oblastí dle odborných způsobilostí:
1) *Zabezpečení dat před zneužitím*, kritérium f) 5 otázek
2) *Ochrana dat před zničením*, zálohování dat, kritérium c) 5 otázek
Testové otázky budou uzavřené, sestavené ze tří odpovědí, z nichž pouze jedna je správná. Všechny otázky jsou bodově rovnocenné.

Autorizovaná osoba zajistí, aby všichni uchazeči plnili test zcela samostatně. V daném termínu před danou zkušební komisí mohou absolvovat test najednou všichni uchazeči. Přítomnost obou členů zkušební komise po celou dobu písemného ověřování je vyžadována.

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „***ústní ověření***":
- jsou ověřována formou individuálního pohovoru obou členů zkušební komise s uchazečem, tj. s vyloučením možnosti, že by odpovědi aktuálně zkoušeného uchazeče slyšel jiný uchazeč / ostatní uchazeči,
- tato kritéria se ověřují například v odděleném samostatném prostoru (místnosti) nebo takovým způsobem, kdy je zaručeno individuální zkoušení uchazeče,
- přítomnost obou členů zkušební komise po celou dobu ústního ověřování je vyžadována.

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „***praktické předvedení a ústní ověření***":
- jsou ověřována tak, že uchazeč nejprve prakticky předvede požadovanou činnost a poté (nikoliv však nutně bezprostředně) na pokyn zkušební komise svou činnost obhájí, odpoví na otázky,
- přítomnost obou členů zkušební komise po celou dobu ověřování formou praktického předvedení a ústního ověření je vyžadována.

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „***praktické předvedení***":
- přítomnost obou členů zkušební komise po celou dobu ověřování formou praktického předvedení je vyžadována.

Specifické pokyny k vybraným odborným způsobilostem a kritériím
K ověření odborné způsobilosti *Sběr dat a analýza údajů v oblasti kybernetické bezpečnosti*, kritérium b) autorizovaná osoba vytvoří 3 případové studie, z nichž si uchazeč při zkoušce vylosuje jednu. Výsledek řešení případové studie zpracuje uchazeč písemně na místě a následně postoupí k ústnímu ověření.

Autorizovaná osoba, resp. autorizovaný zástupce autorizované osoby, je oprávněna předčasně ukončit zkoušku, pokud vyhodnotí, že v důsledku činnosti uchazeče bezprostředně došlo k ohrožení nebo bezprostředně hrozí nebezpečí ohrožení zdraví, života a majetku či životního prostředí. Zdůvodnění předčasného ukončení zkoušky uvede autorizovaná osoba do záznamu o průběhu a výsledku zkoušky. Uchazeč může ukončit zkoušku kdykoliv v jejím průběhu, a to na vlastní žádost.

Výsledné hodnocení

Zkoušející hodnotí uchazeče zvlášť pro každou odbornou způsobilost a výsledek zapisuje do záznamu o průběhu a výsledku zkoušky.

Výsledné hodnocení pro danou odbornou způsobilost musí znít:
- „splnil“, nebo
- „nesplnil“ v závislosti na stanovení závaznosti, resp. nezávaznosti jednotlivých kritérií u každé odborné způsobilosti.

Výsledné hodnocení zkoušky zní buď:
- „vyhověl“, pokud uchazeč splnil všechny odborné způsobilosti, nebo
- „nevyhověl“, pokud uchazeč některou odbornou způsobilost nesplnil. Při hodnocení „nevyhověl“ uvádí autorizovaná osoba vždy zdůvodnění, které uchazeč svým podpisem bere na vědomí.

Počet zkoušejících

Zkouška probíhá před zkušební komisí složenou ze dvou členů. Všichni členové komise musí být přítomni u zkoušky po celou dobu trvání zkoušky.

Zkoušející je povinen provádět ověřování odborných způsobilostí při zkoušce přesně podle všech ustanovení tohoto hodnoticího standardu.

Požadavky na odbornou způsobilost autorizované osoby, resp. autorizovaného zástupce autorizované osoby

Autorizovaná osoba, resp. autorizovaný zástupce autorizované osoby musí splňovat alespoň jednu z následujících variant požadavků:

a) Minimálně střední vzdělání s maturitní zkouškou v oblasti informačních a komunikačních technologií a nejméně 5 let odborné praxe v činnostech pracovníka bezpečnostního dohledového centra informačních systémů.
b) Profesní kvalifikace Pracovník/pracovnice bezpečnostního dohledového centra informačních systémů (18-020-M), střední vzdělání s maturitní zkouškou a nejméně 5 let odborné praxe v činnostech pracovníka bezpečnostního dohledového centra informačních systémů.

Žadatel o udělení autorizace prokazuje splnění požadavků na odbornou způsobilost a praxi v povolání autorizujícímu orgánu, a to předložením dokladu nebo dokladů o získání odborné způsobilosti a praxe v povolání v souladu s hodnoticím standardem této profesní kvalifikace, nebo takovým postupem, který je v souladu s požadavky uvedenými v hodnoticím standardu této profesní kvalifikace autorizujícím orgánem stanoven.

Žádost o udělení autorizace naleznete na internetových stránkách autorizujícího orgánu: Národní úřad pro kybernetickou a informační bezpečnost, www.nukib.gov.cz.

Nezbytné materiální a technické předpoklady pro provedení zkoušky

- Zkušební místnost odpovídající bezpečnostním a hygienickým předpisům se stoly a židlemi, nejlépe specializovaná cyber-sec učebna s možností variabilní konfigurace infrastruktury, zajištěním čisticích a inicializačních procesů a vizualizací stavu,
- psací potřeby, papír,
- soubor testových otázek a zadání případových studií,
- dataprojektor, plátno, flip-chart,

- HW:
  - stolní počítač nebo notebook nebo tablet (dostatečně výkonný, aby zajistil plynulý provoz vyžadovaných aplikací),
  - mobilní telefon (dostatečně výkonný, aby zajistil plynulý provoz vyžadovaných aplikací) pro ověřování kritéria b) odborné způsobilosti *Sběr dat a analýza údajů v oblasti kybernetické bezpečnosti*,
  - internetové připojení,
  - síťový server,
  - cloudové úložiště,

- SW:
  - operační systém Windows/Linux – aktualizovaný v průběhu posledních 3 týdnů,
  - aktualizovaný antivirový program,
  - aktuální kancelářský balík obsahující textový procesor, tabulkový editor, SW pro tvorbu prezentací, e-mailový klient (např. MS Office, nebo LibreOffice),
  - internetový prohlížeč,
  - instalační ISO/DVD s OS Windows a počítač, na který se bude tento OS instalovat (může být virtuální – v tom případě je potřeba mít na zkušebním PC k dispozici virtualizaci, například VMware Player nebo podobnou),
  - instalační ISO/DVD s OS Linux a počítač, na který se bude tento OS instalovat (může být virtuální – v tom případě je potřeba mít na zkušebním PC k dispozici virtualizaci, například VMware player nebo podobnou),
  - software pro sběr a analýzu síťového provozu,
  - nástroj pro ověřování identity, např. Free RADIUS, Open LDAP, Kerberos, Open Diameter,
  - nástroj pro záznam logů např. syslog, syslog-ng, rsyslog,
  - nástroj pro kryptografii např. Open SSL,
  - nástroj pro zajištění úrovně dostupnosti, např. KVM, Open Stack,
  - nástroj pro sběr a vyhodnocení KBU, např. OSSIM/USM od AlienVault, OSSEC.

Uchazeč musí mít na zkušebním zařízení udělena administratorská práva z důvodu dodatečné instalace SW, který používá (zohlednění jeho osobní preference).

K žádosti o udělení autorizace žadatel přiloží seznam materiálně-technického vybavení dokládající soulad s požadavky uvedenými v hodnoticím standardu pro účely zkoušky. Zajištění vhodných prostor pro provádění zkoušky prokazuje žadatel odpovídajícím dokladem (např. výpis z katastru nemovitostí, nájemní smlouva, dohoda).

Doba přípravy na zkoušku

Uchazeč má nárok na celkovou dobu přípravy na zkoušku v trvání 10 minut. Do doby přípravy na zkoušku se nezapočítává doba na seznámení uchazeče s pracovištěm, s organizací zkoušky, s požadavky BOZP a PO a s právy a povinnostmi uchazeče v rámci zkoušky dle zákona č. 179/2006 Sb.

Doba pro vykonání zkoušky

Celková doba trvání vlastní zkoušky jednoho uchazeče (bez času na přestávky a na přípravu) je 5 až 7 hodin (hodinou se rozumí 60 minut). Celková doba trvání písemné části zkoušky jednoho uchazeče je 15 minut.

Autoři standardu

Autoři hodnoticího standardu

Hodnoticí standard profesní kvalifikace připravila SR pro informační technologie a elektronické komunikace, ustavená a licencovaná pro tuto činnost HK ČR a SP ČR.

Na tvorbě se dále podílely subjekty zastoupené v pracovní skupině:

- Network Security Monitoring Cluster, družstvo
- AXENTA, a. s.
- Jihomoravský kraj