Technik/technička kybernetické bezpečnosti (kód: 18-018-N)

Autorizující orgán: Národní úřad pro kybernetickou a informační bezpečnost
Skupina oborů: Informatické obory (kód: 18)
Týká se povolání: Technik kybernetické bezpečnosti
Kvalifikační úroveň NSK - EQF: 5

Odborná způsobilost

Název	Úroveň
Sledování řízení správy a funkčnosti počítačových sítí	5
Uvádění počítačových sítí do provozu a nastavování jejich parametrů	5
Pokročilá instalace operačního systému a jeho konfigurace	6
Konfigurace síťových připojení	4
Orientace v nástrojích používaných v kybernetické bezpečnosti	4
Orientace v administraci IT prostředků	5
Analýza a návrh infrastruktury počítačové sítě, výběr hardware a software pro použití v malé a střední organizaci	4
Virtualizace a cloudová řešení pro malé a střední organizace	5
Monitorování provozu počítačových sítí pro potřeby technika/techničky kybernetické bezpečnosti	5
Monitorování provozu operačních systémů, jejich diagnostika a optimalizace výkonu	4
Zálohování dat a jejich ochrana před zničením nebo zneužitím	5

Platnost standardu

Standard je platný od: 20.05.2025

Kritéria a způsoby hodnocení

Sledování řízení správy a funkčnosti počítačových sítí

Kritéria hodnocení	Způsoby ověření
a) Vyjmenovat alespoň dvě technologie pro provozní monitoring, popsat, jakým způsobem se dá měřit a sledovat výkon sítě a síťových prvků	Ústní ověření
b) Definovat pojem detekce anomálií v provozu sítí, jak lze zvyšovat síťovou bezpečnost proti pokročilým hrozbám (botnety, infikované stanice, DDoS útoky atd.)	Ústní ověření
c) Popsat techniku sledování vytíženosti sítě, určení kritických míst, plánování kapacity sítě	Ústní ověření
d) Uvést příklady útoku na podnikovou síť (ARP spoofing, DDOS, MiTM, session hijacking, …)	Ústní ověření

Je třeba splnit všechna kritéria.

Uvádění počítačových sítí do provozu a nastavování jejich parametrů

Kritéria hodnocení	Způsoby ověření
a) Prokázat znalost ve tvorbě návrhu počítačové sítě včetně návrhu vedení kabelů, umístění síťových prvků, jejich základní konfigurace podle zadání	Písemné ověření
b) Popsat požadavky na dokumentaci počítačové sítě, uvést, které údaje má obsahovat a jak často je třeba dokumentaci aktualizovat	Ústní ověření
c) Vysvětlit použití adresního prostoru, dělení sítě na VLAN, uvést příklady využitelných adresních prostorů	Ústní ověření
d) Vysvětlit vhodné techniky pro použití zabránění kolize IP adres	Ústní ověření
e) Vysvětlit, k čemu se používá DNS (Domain Name Service), k čemu se dají využít vlastní DNS servery v podnikové síti	Ústní ověření

Je třeba splnit všechna kritéria.

Pokročilá instalace operačního systému a jeho konfigurace

Kritéria hodnocení	Způsoby ověření
a) Navrhnout parametry instalace operačního systému Windows/Linux na serveru (např. volba hlavních aplikací – doménový řadič, DNS, DHCP, web server, souborový server, poštovní server, tiskový server) podle zadání	Praktické předvedení a ústní ověření
b) Nakonfigurovat operační systém Windows/Linux na serveru (např. nakonfigurovat parametry sítě a konektivitu do internetu, zavést centrální správu uživatelů, nastavit uživatelské politiky, přiřadit oprávnění uživatelům a skupinám uživatelů) podle zadání	Praktické předvedení a ústní ověření
c) Nakonfigurovat operační systém na klientské stanici (např. přenos profilu, nastavení doménových a lokálních uživatelů a jejich práv, konfigurace uživatelského prostředí)	Praktické předvedení a ústní ověření
d) Popsat a vysvětlit přípravu disků před instalací operačního systému	Ústní ověření
e) Popsat a vysvětlit přípravu hromadných instalací operačního systému na více identických počítačů	Ústní ověření

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.

Orientace v nástrojích používaných v kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Vyjmenovat alespoň 2 nástroje pro ochranu integrity komunikačních sítí a popsat možnosti jejich uplatnění	Ústní ověření
b) Uvést alespoň jeden nástroj pro ověřování identity uživatelů a řízení přístupových oprávnění a popsat možnosti jejich uplatnění	Ústní ověření
c) Vyjmenovat alespoň 3 nástroje pro ochranu před škodlivým kódem a popsat možnosti jejich uplatnění	Ústní ověření
d) Uvést příklady technik pro sledování NetFlow ve vnitřní síti organizace	Ústní ověření
e) Popsat a vysvětlit hlavní funkce SIEM	Ústní ověření
f) Popsat principy kryptografie	Ústní ověření
g) Vysvětlit pojmy symetrický/asymetrický klíč, hashovací funkce, elektronický podpis, časové razítko	Ústní ověření

Je třeba splnit všechna kritéria.

Orientace v administraci IT prostředků

Kritéria hodnocení	Způsoby ověření
a) Uvést příklady internetových komunikačních protokolů, na příkladech vysvětlit jejich použití	Ústní ověření
b) Popsat důležité síťové komponenty (router, switch, DNS, Proxy, firewall) a uvést účel jejich použití a u DNS i způsob zabezpečení	Ústní ověření
c) Prokázat znalost v orientaci v administraci mobilních zařízení a nejrozšířenějších operačních systémů (iOS, Android)	Písemné ověření
d) Popsat základní bezpečnostní protokoly (PKI, TLS, Ipsec, PGP, DNSSEC) a uvést účel jejich použití	Ústní ověření

Je třeba splnit všechna kritéria.

Analýza a návrh infrastruktury počítačové sítě, výběr hardware a software pro použití v malé a střední organizaci

Kritéria hodnocení	Způsoby ověření
a) Analyzovat technické požadavky počítačové sítě, rozhovorem upřesnit detaily (zjistit současný stav z technického, finančního, majetkově-licenčního hlediska); cílem je stručně formulovat návrh na řešení	Praktické předvedení a ústní ověření
b) Navrhnout vhodnou infrastrukturu, HW a SW pro stanice a server podle zadání	Praktické předvedení a ústní ověření
c) Prokázat znalost terminologie, funkce a parametry prostředků z oblasti HW a SW	Písemné ověření

Je třeba splnit všechna kritéria.

Virtualizace a cloudová řešení pro malé a střední organizace

Kritéria hodnocení	Způsoby ověření
a) Vysvětlit principy virtualizace, popsat výhody a nevýhody; navrhnout vhodné řešení podle požadavků zákazníka	Ústní ověření
b) Vysvětlit principy cloudových řešení, popsat výhody a nevýhody. Navrhnout vhodné řešení podle předloženého zadání - požadavků zákazníka	Ústní ověření
c) Nakonfigurovat virtuální server na vybrané virtualizační platformě a spustit na něm vybranou službu (např. elektronická pošta, webový server, sdílení dat, ověřování uživatelů)	Praktické předvedení a ústní ověření

Je třeba splnit všechna kritéria.

Monitorování provozu počítačových sítí pro potřeby technika/techničky kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Popsat způsob provádění měření výkonu síťových prvků a odezvy serveru	Ústní ověření
b) Vysvětlit vlastnosti a využití standardních monitorovacích protokolů (např. SNMP, RMON)	Ústní ověření
c) Aplikovat standardní monitorovací nástroje obsažené v daném operačním systému	Praktické předvedení a ústní ověření
d) Aplikovat standardní diagnostické nástroje z prostředí příkazového řádku obsažené v daném operačním systému	Praktické předvedení a ústní ověření
e) Popsat možnosti terminálového připojení k vzdáleným síťovým prvkům, porovnat jednotlivé technologie (např. Telnet vs. SSH)	Ústní ověření

Je třeba splnit všechna kritéria.

Monitorování provozu operačních systémů, jejich diagnostika a optimalizace výkonu

Kritéria hodnocení	Způsoby ověření
a) Diagnostikovat stav a vytíženost hardwarových systémových prostředků pomocí nástrojů operačního systému (např. sledování teploty procesoru, spotřeby paměti, vytížení procesoru, zápisu na disk)	Praktické předvedení a ústní ověření
b) Kontrolovat systémové logy, identifikovat kritické události, sledovat logy z více serverů a analyzovat je	Praktické předvedení a ústní ověření
c) Analyzovat chyby a nefunkčnosti operačních systémů; vyhledat s pomocí dostupných zdrojů řešení problému na stránkách výrobců nebo odborně zaměřených portálů. Porozumět nalezenému řešení v angličtině; implementovat nalezené řešení	Praktické předvedení a ústní ověření
d) Ověřit funkčnost jednotlivých hardwarových komponent; vyřešit jednoduchý problém (např. tiskárna netiskne, PC nebootuje)	Praktické předvedení a ústní ověření

Je třeba splnit všechna kritéria.

Zálohování dat a jejich ochrana před zničením nebo zneužitím

Kritéria hodnocení	Způsoby ověření
a) Navrhnout postupy a způsob zálohování databáze, popsat, jaký interval zvolit, jaký typ zálohy (kompletní, inkrementální, rozdílová)	Praktické předvedení a ústní ověření
b) Popsat vhodné ukládání záloh, jaká zařízení, za jakých podmínek mohou být připojeny k zálohovanému systému	Ústní ověření
c) Vysvětlit rozdíl mezi on-line a off-line zálohami	Ústní ověření
d) Vysvětlit a rozebrat výhody/nevýhody následujících médií pro ukládání záloh: magnetická páska, pevný disk, NAS, optický disk, vzdálená zálohovací služba	Ústní ověření
e) Navrhnout a popsat způsob obnovy zálohované databáze	Praktické předvedení a ústní ověření

Je třeba splnit všechna 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 podle zákona č. 179/2006 Sb., a s požadavky bezpečnosti a ochrany zdraví při práci (BOZP) a požární ochrany (PO), o čemž autorizovaná osoba vyhotoví a uchazeč podepíše 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 provedení 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 (rozsah 30 min., 15 otázek)

Pravidla pro aplikaci písemného 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 45 testových otázek, zaměřených na ověření znalostní složky vybraných odborných způsobilostí:

- *Uvádění počítačových sítí do provozu a nastavování jejich parametrů*, kritérium a) 15 otázek
- *Orientace v administraci IT prostředků*, kritérium c) 15 otázek
- *Analýza a návrh infrastruktury počítačové sítě, výběr hardware a software pro použití v malé a střední organizaci*, kritérium c) 15 otázek

Autorizovaná osoba zajistí vygenerování náhodného testu pro každého uchazeče, sestaveného z 15 otázek s následujícím zastoupením jednotlivých oblastí podle odborných způsobilostí:
1) *Uvádění počítačových sítí do provozu a nastavování jejich parametrů*, kritérium a) 5 otázek
2) *Orientace v administraci IT prostředků*, kritérium c) 5 otázek
3) *Analýza a návrh infrastruktury počítačové sítě, výběr hardware a software pro použití v malé a střední organizaci*, 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 zkoušejícího po celou dobu písemného ověřování je vyžadována.

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „***ústní ověření***":
- jsou ověřována formou individuálního pohovoru zkoušejícího 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 zkoušejícího 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 zkoušejícího svou činnost obhájí, odpoví na otázky,
- přítomnost zkoušejícího po celou dobu ověřování formou praktického předvedení a ústního ověření je vyžadována.

Autorizovaná osoba, resp. autorizovaný zástupce autorizované osoby je oprávněný 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 jedním zkoušejícím, který musí být přítomen u zkoušky po celou dobu jejího trvání.

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) Nejméně vyšší odborné vzdělání v oblasti informačních a komunikačních technologií a nejméně 5 let prokázané odborné praxe v činnostech technika kybernetické bezpečnosti.
b) Profesní kvalifikace Technik/technička kybernetické bezpečnosti (18-018-N) a alespoň vyšší odborné vzdělání a nejméně 5 let prokázané odborné praxe v činnostech technika kybernetické bezpečnosti.

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, stoly, židle,
- psací potřeby, papír,
- dataprojektor, plátno, flip-chart,
- připravený soubor testových otázek a případových studií,

- HW:
  - stolní počítač nebo notebook nebo tablet (dostatečně výkonný natolik, aby zajistil plynulý provoz vyžadovaných aplikací),
  - mobilní telefon (dostatečně výkonný, aby zajistil plynulý provoz vyžadovaných aplikací) pro ověřování prakticky ověřovaných kritérií odborné způsobilosti *Monitorování provozu operačních systémů, jejich diagnostika a optimalizace výkonu,*
  - 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,
  - zálohovací software pro praktické předvedení (Veeam, Acronic Cyber Backup)
  - 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 Stac,
  - nástroj pro sběr a vyhodnocení KBU, např. OSSIM/USM od AlienVault, OSSEC.

Uchazeč musí mít na zkušebním zařízení udělena administrátorská práva z důvodu doplnění 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 podle zákona č. 179/2006 Sb.

Doba pro vykonání zkoušky

Celková doba trvání vlastní zkoušky jednoho uchazeče (bez času na přípravu a přestávky) je 9 až 10 hodin (hodinou se rozumí 60 minut). Celková doba trvání písemné části zkoušky jednoho uchazeče je 30 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