Manažer/manažerka kybernetické bezpečnosti (kód: 18-015-T)

Autorizující orgán: Národní úřad pro kybernetickou a informační bezpečnost
Skupina oborů: Informatické obory (kód: 18)
Týká se povolání: Manažer kybernetické bezpečnosti
Kvalifikační úroveň NSK - EQF: 7

Odborná způsobilost

Název	Úroveň
Orientace v legislativě v oblasti kybernetické bezpečnosti pro potřeby manažera/manažerky kybernetické bezpečnosti	7
Uplatňování principů řízení kybernetické bezpečnosti	7
Supervize dokumentace řízení kybernetické bezpečnosti v organizaci	7
Řízení aktiv v kybernetické bezpečnosti	7
Řízení rizik kybernetické bezpečnosti pro potřeby manažera/manažerky kybernetické bezpečnosti	7
Zajištění organizační bezpečnosti v oblasti kybernetické bezpečnosti	7
Řízení rozvoje bezpečnostního povědomí organizace v oblasti kybernetické bezpečnosti	7
Řízení dodavatelů v oblasti kybernetické bezpečnosti	7
Řízení provozu a komunikací v oblasti kybernetické bezpečnosti	7
Řízení změn v rámci kybernetické bezpečnosti	7
Řízení přístupu a identit v oblasti kybernetické bezpečnosti	7
Zajištění bezpečnosti v oblasti akvizice, vývoje a údržby kybernetické bezpečnosti	7
Vyhodnocování bezpečnostních a provozních událostí v oblasti kybernetické bezpečnosti	7
Koordinace řízení kybernetických bezpečnostních incidentů	7
Zajišťování fyzické bezpečnosti v oblasti kybernetické bezpečnosti	7
Řízení bezpečnostních opatření v oblasti ochrany před škodlivým kódem v oboru kybernetické bezpečnosti	7
Řízení kontinuity činností	7

Platnost standardu

Standard je platný od: 20.05.2025

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 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 hodnotícím 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 45 minut, 20 otázek).
Pravidla pro aplikaci testů:
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 60 otázek, z nichž náhodným výběrem zvolí 20 testových otázek zaměřených na ověření znalostní složky vybrané odborné způsobilosti:

- *Uplatňování principů řízení kybernetické bezpečnost*i, kritérium a) 10 otázek z 30
- *Zajištění organizační bezpečnosti v oblasti kybernetické bezpečnosti*, kritérium a) 10 otázek z 30

Testové otázky budou uzavřené, sestavené ze tří variant 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 „***písemné ověření a ústní ověření***":
Autorizovaná osoba vypracuje soubor 35 zadání určených pro splnění následujících kritérií ve složení:

- *Uplatňování principů řízení kybernetické bezpečnosti*, kritérium b) 5 zadání
- *Uplatňování principů řízení kybernetické bezpečnosti*, kritérium d) 5 zadání
- *Řízení aktiv v kybernetické bezpečnosti*, kritérium a) 5 zadání
- *Zajištění organizační bezpečnosti v oblasti kybernetické bezpečnosti*, kritérium b) 5 zadání
- *Řízení rozvoje bezpečnostního povědomí organizace v oblasti kybernetické bezpečnosti*, kritérium a) 5 zadání
- *Řízení rozvoje bezpečnostního povědomí organizace v oblasti kybernetické bezpečnosti*, kritérium b) 5 zadání
- *Koordinace řízení kybernetických bezpečnostních incidentů*, kritérium b) 5 zadání

Autorizovaná osoba zajistí náhodný výběr jednoho zadání pro každé z výše uvedených kritérií.
Uchazeč podle zadání vypracuje písemnou odpověď a obhájí ji v ústním ověření. Na vypracování písemných odpovědí má uchazeč 40 minut.

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 jsou ověřována prostřednictvím případové studie. Autorizovaná osoba vytváří celkem 10 případových studií, z nichž si uchazeč jednu vylosuje a ve kterých je vždy uvedeno:
  - předmět činnosti fiktivní organizace,
  - strategie rozvoje ICT organizace s uvedením priorit na další účetní období,
  - organizační struktura organizace,
  - charakteristiky útvaru, kde má být proveden audit,
  - definici informační a komunikační infrastruktury organizace,
  - přehled primárních a podpůrných aktiv organizace s uvedením vazeb.

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.

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.

Autoři standardu

Autoři kvalifikačního standardu

Kvalifikační 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