

## Architekt/architektka kybernetické bezpečnosti (kód: 18-017-T)

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

### Odborná způsobilost

Název	Úroveň
Orientace v legislativě v oblasti kybernetické bezpečnosti	7
Uplatňování principů návrhu architektury informačních systémů se zohledněním požadavků kybernetické bezpečnosti	7
Orientace v pojmech a definicích z oblasti návrhu architektury informačních systémů	7
Kapacitní plánování při návrhu architektury kybernetické bezpečnosti	7
Začlenění řízení rizik do architektury kybernetické bezpečnosti	7
Uplatnění technických bezpečnostních prvků (security devices) v architektuře informačních systémů	7
Principy návrhu bezpečné architektury ICT	7
Principy realizace jednotlivých bezpečnostních opatření podle zákona o kybernetické bezpečnosti	7

### Platnost standardu

Standard je platný od: 20.05.2025

## Kritéria a způsoby hodnocení

### Orientace v legislativě v oblasti kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Popsat význam a vysvětlit členění zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů	Ústní ověření
b) Popsat a vysvětlit prováděcí předpisy vztahující se k zákonu č. 181/2014 Sb. (vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury), ve znění pozdějších předpisů	Ústní ověření
c) Definovat legislativní rámec pro vyspecifikovanou povinnou osobu v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů	Ústní ověření

Je třeba splnit všechna kritéria.

### Uplatňování principů návrhu architektury informačních systémů se zohledněním požadavků kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Popsat principy a procesy řízení architektury kybernetické bezpečnosti podle metodik publikovaných NÚKIB	Písemné ověření
b) Vysvětlit zásady návrhu architektury kybernetické bezpečnosti	Ústní ověření
c) Vysvětlit vedení dokumentace IS a služeb ICT v modelech, které jsou v souladu se standardy TOGAF a ArchiMate	Ústní ověření

Je třeba splnit všechna kritéria.

### Orientace v pojmech a definicích z oblasti návrhu architektury informačních systémů

Kritéria hodnocení	Způsoby ověření
a) Aplikovat pojmy z oblasti procesní architektury (firemní procesy, datové toky) dle konkrétního zadání	Praktické předvedení a ústní ověření
b) Prokázat orientaci v pojmech a procesech CSIRT týmů (ve smyslu RFC 2350)	Písemné ověření

Je třeba splnit obě kritéria.

### Kapacitní plánování při návrhu architektury kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Prokázat orientaci v oblasti řízení finančních zdrojů (stanovení rozpočtu dle potřeby prioritizace realizačních projektů a rozdělení na etapy)	Písemné ověření
b) Prokázat orientaci v základních pojmech z oblasti řízení lidských zdrojů (alokace lidských zdrojů dle potřeby prioritizace realizačních projektů a rozdělení na etapy)	Písemné ověření
c) Identifikovat požadavky na zajištění kybernetické bezpečnosti a aplikovat jednotlivé požadavky do návrhu architektury kybernetické bezpečnosti	Praktické předvedení a ústní ověření

**Je třeba splnit všechna kritéria.**

### Začlenění řízení rizik do architektury kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Popsat analýzu rizik dle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů	Ústní ověření
b) Prokázat orientaci v principech stanovení aktiv včetně určení jejich hodnoty, hrozeb, zranitelností, dopadů, odpovědností a opatření v rámci kybernetické bezpečnosti dle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů	Písemné ověření
c) Aplikovat vybranou metodu řízení rizik do návrhu architektury kybernetické bezpečnosti	Praktické předvedení a ústní ověření

**Je třeba splnit všechna kritéria.**

### Uplatnění technických bezpečnostních prvků (security devices) v architektuře informačních systémů

Kritéria hodnocení	Způsoby ověření
a) Specifikovat a navrhnout nástroje pro ochranu integrity komunikačních sítí a popsat možnosti jejich uplatnění	Praktické předvedení a ústní ověření
b) Specifikovat nástroje pro ověřování identity uživatelů a řízení přístupových oprávnění a popsat možnosti jejich uplatnění	Ústní ověření
c) Specifikovat nástroje pro ochranu před škodlivým kódem a popsat možnosti jejich uplatnění	Ústní ověření
d) Specifikovat nástroje pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů a popsat možnosti jejich uplatnění	Ústní ověření
e) Specifikovat nástroje pro detekci kybernetických bezpečnostních událostí a nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí a popsat možnosti jejich uplatnění	Ústní ověření
f) Specifikovat kryptografické prostředky a popsat možnosti jejich uplatnění	Ústní ověření

**Je třeba splnit všechna kritéria.**

### Principy návrhu bezpečné architektury ICT

Kritéria hodnocení	Způsoby ověření
a) Popsat jednotlivé topologie počítačových sítí a jejich výhody a nevýhody při tvorbě bezpečné architektury. Navrhnout vhodnou topologii počítačové sítě	Praktické předvedení a ústní ověření
b) Vyjmenovat a popsat druhy komunikačních protokolů a jejich základní specifikace	Ústní ověření
c) Popsat principy logické a fyzické stavby sítě	Ústní ověření
d) Popsat metody ověřování úrovně bezpečnosti systému – audit, penetrační testy, zátěžové testy, typická selhání a reakce na ně v oblasti architektury systému	Ústní ověření

**Je třeba splnit všechna kritéria.**

### Principy realizace jednotlivých bezpečnostních opatření podle zákona o kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Popsat obecně platný přístup k implementaci bezpečnostních opatření podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (přístup na základě analýzy rizik, přiměřenosti)	Ústní ověření
b) Vysvětlit princip kontinuálního zlepšování a plánování	Ústní ověření
c) Dle konkrétního zadání vyjmenovat a popsat aplikaci alespoň pěti vhodných technických opatření podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat	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 započítáním 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 obsahujícím 60 otázek a trvajícím 120 minut.

Pravidla pro aplikaci testů:

Soubor otázek pro testy stanovuje autorizovaná osoba podle požadavků hodnoticího standardu.

Musí přitom být splněna 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 180 testových otázek, zaměřených na ověření znalostní složky vybraných odborných způsobilostí:

- *Orientace v legislativě z oblasti kybernetické bezpečnosti* - 30 otázek
- *Uplatňování principů návrhu architektury informačních systémů se zohledněním požadavků kybernetické bezpečnosti* - 30 otázek
- *Orientace v pojmech a definicích z oblasti návrhu architektury informačních systémů* - 60 otázek
- *Kapacitní plánování při návrhu architektury kybernetické bezpečnosti* - 30 otázek
- *Začlenění řízení rizik do architektury kybernetické bezpečnosti* - 30 otázek

Autorizovaná osoba zajistí vygenerování náhodného testu pro každého uchazeče, sestaveného z 60 otázek s následujícím zastoupením jednotlivých oblastí dle odborných způsobilostí:

- *Orientace v legislativě z oblasti kybernetické bezpečnosti* - 10 otázek
- *Uplatňování principů návrhu architektury informačních systémů se zohledněním požadavků kybernetické bezpečnosti* - 10 otázek
- *Orientace v pojmech a definicích z oblasti návrhu architektury informačních systémů* - 20 otázek
- *Kapacitní plánování při návrhu architektury kybernetické bezpečnosti* - 10 otázek
- *Začlenění řízení rizik do architektury kybernetické bezpečnosti* - 10 otázek

Testové otázky budou uzavřené, sestavené ze tří odpovědí, z nichž pouze jedna je správná. Všechny otázky jsou bodově rovnocenné.

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.

#### **Specifické pokyny k vybraným odborným způsobilostem a kritériím:**

K ověření odborné způsobilosti *Kapacitní plánování při návrhu architektury kybernetické bezpečnosti*, kritérium c) 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 hodnotícího standardu.

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

Autorizovaná osoba, resp. autorizovaný zástupce autorizované osoby musí splňovat tento požadavek:

Vysokoškolské vzdělání magisterského stupně, vyškolení dle požadavků vyškolení dle požadavků § 7 a přílohy č. 6 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů (např. certifikace uvedené v příloze č. 6 vyhlášky) a nejméně 5 let prokázané odborné praxe v činnostech architekta 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 hodnotícím standardem této profesní kvalifikace, nebo takovým postupem, který je v souladu s požadavky uvedenými v hodnotícím 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](http://www.nukib.gov.cz).

## Nezbytné materiální a technické předpoklady pro provedení zkoušky

- Učebna odpovídající bezpečnostním a hygienickým předpisům, stoly, židle,
- psací potřeby, papír,
- soubor testových otázek a soubor 3 případových studií,
- stolní počítač nebo notebook (dostatečně výkonný natolik, aby zajistil plynulý provoz aplikací) s aktuálním operačním systémem, kancelářský software, internetové připojení,
- dataprojektor, plátno, flip-chart.

K žádosti o udělení autorizace žadatel přiloží seznam materiálně-technického vybavení dokládající soulad s požadavky uvedenými v hodnotícím 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 7 až 9 hodin (hodinou se rozumí 60 minut). Celková doba trvání písemné části zkoušky jednoho uchazeče je 120 minut.

## **Autoři standardu**

### **Autoři hodnotícího standardu**

Hodnotící 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