NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Certifikačná schéma overovania odbornej spôsobilosti audítora kybernetickej bezpečnosti

Verzia 3.6 zo dňa 27.12.2024 účinná od 1.1.2025

1 TERMÍNY A DEFINÍCIE

Termín	Význam
akreditácia	osvedčenie treťou stranou týkajúce sa orgánu posudzovania zhody, ktorým sa formálne potvrdzuje jeho kompetentnosť, nestrannosť a konzistentné fungovanie v rámci konkrétnych činností posudzovania zhody (STN EN ISO/IEC 17000: 2022)
audit	systematický, nezávislý a zdokumentovaný proces získavania záznamov, konštatovaní faktov alebo iných dôležitých informácií a ich objektívneho posudzovania s cieľom určiť rozsah, v akom sa splnili určené požiadavky (ISO/IEC 17024:2012)
autorizácia	vládne splnomocnenie orgánu posudzovania zhody vykonávať určené činnosti posudzovania zhody (STN EN ISO/IEC 17000: 2022)
certifikačné požiadavky	súbor stanovených požiadaviek, vrátane požiadaviek schémy, ktoré je potrebné splniť, na preukázanie alebo udržanie certifikácie (ISO/IEC 17024:2012)
certifikačný orgán	orgán vykonávajúci posudzovanie zhody treťou stranou podľa certifikačnej schémy (ISO/IEC 17024:2012)
certifikačný proces	činnosti, na základe ktorých certifikačný orgán určí, že osoba spĺňa certifikačné požiadavky , zahŕňa podanie žiadosti, posúdenie, rozhodnutie o certifikácii, recertifikácii a používanie certifikátov, loga a certifikačných značiek (ISO/IEC 17024:2012)
certifikát	dokument vydaný certifikačným orgánom v súlade s ustanoveniami tejto medzinárodnej normy, osvedčujúci, že menovaná osoba splnila certifikačné požiadavky (ISO/IEC 17024:2012)
dohľad	systematické opakovanie činností posudzovania zhody ako základ udržania platnosti potvrdenia o zhode (STN EN ISO/IEC 17000: 2022)
dozor	osoba poverená certifikačným orgánom, ktorá pomáha dohliadať alebo dohliada na skúšku, ale nehodnotí kompetentnosť kandidáta
kandidát	žiadateľ, ktorý splnil stanovené predpoklady a bol zaradený do certifikačného procesu (ISO/IEC 17024:2012)
kvalifikácia	preukázané vzdelanie, odborná príprava a pracovné skúsenosti
objekt posudzovania zhody	akýkoľvek konkrétny materiál, produkt, inštalácia, proces, systém, osoba alebo orgán, ktorých sa týka posudzovanie zhody (ISO/IEC 17065: 2013, ISO/IEC 17021-1:2015, ISO/IEC 17024:2012)
odvolanie sa	žiadosť žiadateľa, kandidáta alebo certifikovanej osoby o opätovné zváženie akéhokoľvek rozhodnutia certifikačného orgánu, ktoré sa týka ním požadovaného stavu certifikácie (ISO/IEC 17024:2012)
orgán posudzovania zhody	orgán, ktorý vykonáva služby posudzovania zhody (ISO/IEC 17024:2012)
osvedčovanie	vydanie vyhlásenia na základe rozhodnutia, o tom, že bolo preukázané splnenie určených požiadaviek (STN EN ISO/IEC 17000: 2022)
posudzovanie	proces, ktorým sa hodnotí ako konkrétna osoba splnila požiadavky certifikačnej schémy (ISO/IEC 17024:2012)
posudzovanie zhody	preukázanie splnenia určených požiadaviek (STN EN ISO/IEC 17000: 2022)
skúšajúci	kompetentná osoba na vykonávanie a klasifikovanie skúšky, ak skúška vyžaduje odborné hodnotenie

Termín	Význam
skúšanie (testovanie)	určenie jednej alebo viacerých vlastností predmetu posudzovania zhody podľa postupu. Termín skúšanie sa zvyčajne týka materiálov, produktov alebo procesov. V niektorých aplikačných oblastiach sa uprednostňuje z angličtiny prevzatý termín testovanie, resp. test (napr. testovanie hypotéz, testovanie softvéru a pod.). (ISO/IEC 17000: 2022)
skúška	mechanizmus tvoriaci časť posudzovania, ktorým sa hodnotí kompetentnosť kandidáta jedným alebo viacerými spôsobmi, ako písomne, ústne, prakticky alebo pozorovaním, podľa nadefinovania v certifikačnej schéme
spôsobilosť	schopnosť uplatniť vedomosti a zručnosti na dosiahnutie zamýšľaných výsledkov
sťažnosť	vyjadrenie nespokojnosti, inej ako v odvolaní, predložené certifikačnému orgánu jednotlivcom alebo organizáciou, vo veci činností tohto orgánu alebo certifikovanej osoby, s očakávaním odpovede (ISO/IEC 17024:2012)
špecifikácia spôsobilostí	normatívny dokument definujúci kritériá spôsobilosti
vlastník schémy	organizácia zodpovedná za rozvoj a udržiavanie certifikačnej schémy (ISO/IEC 17024:2012)
žiadateľ	osoba, ktorá podala žiadosť o prijatie do certifikačného procesu (ISO/IEC 17024:2012)

2 ÚVOD

2.1 ROZSAH CERTIFIKÁCIE

Predmet certifikácie	Audítor kybernetickej bezpečnosti podľa osobitných predpisov[1)]
Opis práce a úloh	Preverenie účinnosti prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a k nemu vydaných vykonávacích predpisov vykonaním auditu kybernetickej bezpečnosti.

2.2 PRÁVNY ZÁKLAD A NORMATÍVNE KRITÉRIÁ

Táto certifikačná schéma sa opiera najmä o nasledujúcu právnu úpravu a technické normy:

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“);
- Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v kybernetickej bezpečnosti (ďalej len „vyhláška č. 492/2022 Z. z.“);
- Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti;
- Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.“);

[1)] § 29 ods. 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

- Zákon č. 56/2018 Z. z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu a o zmene
  a doplnení niektorých zákonov v znení zákona č. 259/2021 Z. z. (ďalej len „zákon č. 56/2018“);
- ISO/IEC 17024:2012 Posudzovanie zhody - Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb;
- ISO/IEC 17000:2022 Posudzovanie zhody - Slovník a všeobecné zásady.

Pokiaľ nie je uvedená verzia dokumentu, všetky vyššie uvedené právne predpisy a technické normy sú citované v znení ich platnej verzie.

2.3 CERTIFIKAČNÉ ROLY

2.3.1 Vlastník certifikačnej schémy

Certifikačnú schému overovania odbornej spôsobilosti audítora vydáva **Národný bezpečnostný úrad (ďalej len „NBÚ“)**, ako orgán dohľadu v oblasti kybernetickej bezpečnosti. Táto certifikačná schéma stanovuje postup pri certifikácii audítora kybernetickej bezpečnosti.

2.3.2 Orgány posudzovania zhody

V záujme zachovania kvality určuje certifikačná schéma certifikačné procesy, všeobecné a osobitné požiadavky na certifikáciu audítora kybernetickej bezpečnosti. Služby posudzovania zhody vykonávajú **orgány posudzovania zhody** podľa tejto certifikačnej schémy a podľa odporúčaní medzinárodne akceptovaných štandardov alebo iných vecne obdobných postupov príslušným na certifikáciu personálu.

Orgán posudzovania zhody vydávajúci certifikáty založené na tejto certifikačnej schéme musí spĺňať požiadavky medzinárodnej normy ISO/IEC 17024.

Orgánom posudzovania zhody vydávajúcim certifikáty založených na tejto certifikačnej schéme môže byť len orgán verejnej správy podľa osobitného predpisu.[2]

2.3.3 Akreditačný orgán

Vnútroštátny **akreditačný orgán** je jediný orgán v členskom štáte Európskej únie (EÚ), ktorý vykonáva akreditáciu na základe právomoci, ktorú mu udelil štát. V Slovenskej republike je vnútroštátnym akreditačným orgánom Slovenská národná akreditačná služba (ďalej ako „SNAS“). Postavenie SNAS a jej pôsobnosť určuje zákon č. 53/2023 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Orgán posudzovania zhody je oprávnený vydávať certifikát audítora kybernetickej bezpečnosti len za predpokladu, že je na to akreditovaný SNAS pre oblasť certifikácie osôb v súlade s touto certifikačnou schémou.

[2]) § 3 ods. 1 zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

3 KRITÉRIÁ CERTIFIKÁCIE

3.1 VŠEOBECNÉ POŽIADAVKY NA SPÔSOBILOSŤ

3.1.1 Minimálne všeobecné požiadavky na spôsobilosť

Od kandidáta sa vyžaduje znalosť auditu kybernetickej bezpečnosti alebo informačnej bezpečnosti, alebo auditu informačných systémov, ktorá sa preukazuje certifikátom audítora podľa technickej normy[3]) alebo ekvivalentným medzinárodným osvedčením o spôsobilosti vykonávať audit informačnej, alebo kybernetickej bezpečnosti.

3.1.2 Minimálne požiadavky na vzdelanie a prax

Minimálne požiadavky na úroveň vzdelania a prax žiadateľa o overenie odbornej spôsobilosti:

Vzdelanie a požadovaný doklad	Prax a spôsob jej preukázania (alternatívy predložených dokumentov)
Úplné stredné všeobecné vzdelanie alebo úplné stredné odborné vzdelanie (doklad o získanom stupni vzdelania a o získanej kvalifikácii)	prax v oblasti informačných technológií, kybernetickej bezpečnosti - najmenej 10 rokov praxe (životopis s uvedením kontaktu na overiteľnú referenciu, zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu), z toho skúsenosti v oblasti auditu informačných systémov - najmenej 7 rokov praxe (medzinárodný certifikát, alebo ekvivalentné osvedčenie z oblasti auditu informačných systémov, zoznam vykonaných auditov v roli audítora alebo vedúceho audítora s uvedením kontaktu na overiteľnú referenciu, zoznam vykonaných auditov v roli audítora v tréningu s uvedením kontaktu na vedúceho audítora, ktorý audit viedol)
Vysokoškolské vzdelanie prvého stupňa (doklady o absolvovaní štúdia)	skúsenosti v oblasti informačných technológií, kybernetickej bezpečnosti - najmenej 7 rokov praxe (životopis s uvedením kontaktu na overiteľnú referenciu, zoznam auditov), z toho skúsenosti v oblasti auditu informačných systémov - najmenej 5 rokov praxe (medzinárodný certifikát, alebo ekvivalentné osvedčenie z oblasti auditu informačných systémov, zoznam vykonaných auditov v roli audítora alebo vedúceho audítora s uvedením kontaktu na overiteľnú referenciu, zoznam vykonaných auditov v roli audítora v tréningu s uvedením kontaktu na vedúceho audítora, ktorý audit viedol)
Vysokoškolské vzdelanie druhého a tretieho stupňa (doklady o absolvovaní štúdia)	skúsenosti v oblasti informačných technológií, kybernetickej bezpečnosti - najmenej 5 rokov praxe (životopis s uvedením kontaktu na overiteľnú referenciu, zoznam auditov), z toho skúsenosti v oblasti auditu informačných systémov - najmenej 3 roky praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT alebo regulácie kybernetickej bezpečnsoti na ústrednom orgáne štátnej správy pre kybernetickú bezpečnosť (medzinárodný certifikát, alebo ekvivalentné osvedčenie z oblasti auditu informačných systémov, zoznam vykonaných auditov v roli audítora alebo vedúceho audítora s uvedením kontaktu na overiteľnú referenciu, zoznam vykonaných auditov v roli audítora v tréningu s uvedením kontaktu na vedúceho audítora, ktorý audit viedol)

[3]) ISO/IEC 27001

3.1.3 Predpoklady na výkon činnosti audítora

- **nezávislosť** - audítor je nezávislý pri posudzovaní bezpečnostných opatrení, ak sa počas posledných troch rokov pred konaním auditu nezúčastňoval na riadení alebo prevádzke auditovaných informačných systémov; dokladá sa vyhlásením pri každom audite,
- **objektívnosť** - za objektívneho sa považuje ten, u koho neboli uznané sťažností na objektívnosť počas vykonávanej praxe,
- **bezúhonnosť** – za bezúhonného sa na účely tejto schémy nepovažuje ten, kto bol v posledných 10 rokoch právoplatne odsúdený za niektorý z trestných činov uvedených v § 247 až § 247d zákona č. 300/2005 Z. z. Trestného zákona.

3.1.4 Špecifické kľúčové kompetencie

Od kandidáta sa vyžadujú nasledujúce osobnostné požiadavky a schopnosti:

- schopnosť prijímať rozhodnutia,
- schopnosť myslieť a konať v súvislostiach,
- schopnosť poskytovať spätnú väzbu,
- schopnosť delegovať úlohy,
- schopnosť viesť pracovný tím,
- schopnosť organizovania a plánovania práce,
- analytické myslenie,
- tvorivosť (kreativita),
- prezentačná zručnosť.

3.2 OSOBITNÉ POŽIADAVKY NA SPÔSOBILOSŤ

Od kandidáta sa vyžadujú nasledujúce minimálne požiadavky - **vedomosti** na úroveň odbornej spôsobilosti audítora pre proces auditu kybernetickej bezpečnosti:

1. Znalosť procesov a systému riadenia informačnej a kybernetickej bezpečnosti.
2. Znalosť zásad organizácie informačnej a kybernetickej bezpečnosti.
3. Znalosť zásad personálnej bezpečnosti.
4. Znalosť zásad riadenia prístupov a identít.
5. Znalosti o spôsobe používania kryptografických bezpečnostných mechanizmov.
6. Znalosť princípov testovania kybernetickej bezpečnosti.
7. Znalosť zásad auditu kybernetickej bezpečnosti.
8. Znalosť právnych predpisov, požiadaviek na súlad a noriem vzťahujúcich sa na kybernetickú bezpečnosť, najmä:
   - smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii,
   - smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii,
   - nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu,
   - zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
   - vyhlášky NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
   - vyhlášky NBÚ č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
   - vyhlášky NBÚ č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v kybernetickej bezpečnosti,

- vyhlášky NBÚ č. 493/2022 Z. z. o audite kybernetickej bezpečnosti,
- zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o doplnení niektorých zákonov,
- zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov,
- zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov,
- medzinárodných noriem z ISO/IEC 27000 „Informačné technológie - Bezpečnostné metódy - Systémy riadenia informačnej bezpečnosti“,
- medzinárodných noriem z ISA/IEC 62443 „Security for Industrial Automation and Control Systems“.

9. Znalosť právnych predpisov a požiadaviek na súlad vzťahujúcich sa na ochranu osobných údajov, najmä:
   - nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
   - zákona č. 18/2018 Z. z. o ochrane osobných údajov a o doplnení niektorých zákonov,
10. Znalosť štandardov a zásad ochrany osobných údajov, vrátane metodických usmernení Úradu na ochranu osobných údajov Slovenskej republiky,
11. Znalosť procesov a metodík riadenia rizík.
12. Znalosť postupov analýzy rizík.
13. Znalosť typických hrozieb a postupov pre identifikáciu hrozieb a zraniteľností.
14. Znalosť bezpečnostných mechanizmov.
15. Znalosť metodík podnikovej architektúry.
16. Znalosť procesov riešenia kybernetických bezpečnostných incidentov.
17. Znalosť princípov plánovania havarijnej obnovy prevádzky.
18. Znalosť procesov riadenia kontinuity činností a princípov plánovania havarijnej obnovy.
19. Znalosť princípov logovania a bezpečnostného monitorovania.
20. Znalosť zásad riadenia fyzickej a objektovej bezpečnosti.
21. Znalosť na mechanizmov vo fyzickej a objektovej bezpečnosti.
22. Znalosť princípov riadenia služieb v oblasti informačných technológií .
23. Znalosť princípov riadenia nákladov a rozpočtových pravidiel.
24. Znalosť princípov riadenia ľudských zdrojov.
25. Znalosť konceptov počítačových sietí.
26. Znalosť zásad riadenia projektov.
27. Znalosť zásad riadenia dodávateľských služieb.
28. Znalosť zásad navrhovania a vývoja aplikácií a informačných systémov.
29. Znalosť zásad obstarávania informačných systémov.
30. Znalosť zásad aplikačnej bezpečnosti.
31. Znalosť princípov a procesov auditovania.
32. Technické vedomosti o auditovaných systémoch.
33. Znalosť metód posudzovania rizík dostatočná pre vyhodnotenie rizík auditu a posúdenia hodnotenia rizík, kategorizácie informačných systémov prevádzkovateľov.

4 POSÚDENIE ZHODY

Posúdenie spôsobilosti kandidátov podľa tejto schémy má za cieľ overiť a potvrdiť, že boli dosiahnuté požiadavky na kvalifikáciu audítora podľa Vyhlášky NBÚ č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v kybernetickej bezpečnosti a Vyhlášky NBÚ č. 493/2022 Z. z. o audite kybernetickej bezpečnosti s príslušnými spôsobilosťami, ktoré umožnia audítorom samostatne posudzovať zhodu subjektov s požiadavkami Vyhlášky NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a to:

4.1 POČIATOČNÉ KRITÉRIÁ CERTIFIKÁCIE

Ako predpoklad počiatočnej certifikácie musí orgán posudzovania zhody vyžadovať objektívne dôkazy o tom, že osoba, ktorá žiada o certifikáciu, spĺňa základné požiadavky týkajúce sa profilu uvedené v príslušnej špecifikácii spôsobilosti. Orgán posudzovania zhody je zodpovedný za identifikáciu vhodných referenčných úrovní v rámci príslušného kontextu národnej kvalifikácie a odbornej prípravy.

Predpoklady počiatočnej certifikácie zahŕňajú najmä:

- príslušné vzdelanie,
- prax a rozsah všeobecných pracovných skúseností,
- formálne školenia a odborné certifikáty,
- audítorské skúsenosti,
- plnenie požiadaviek kódexu profesionálneho správania audítora kybernetickej bezpečnosti (etický kódex).

v kontexte systému hodnotenia a certifikácie riadeného v súlade s pravidlami akreditačného orgánu v členskom štáte EÚ, pod dohľadom akreditačného orgánu členského štátu.

Osvedčenia, ktorými je potvrdené splnenie všetkých týchto podmienok, sa na účely tejto schémy nazývajú „certifikáty“.

4.2 POSUDZOVANIE ŽIADATEĽOV

Posúdenie sa vykonáva plánovaným a štruktúrovaným spôsobom, ktorý zabezpečí, aby požiadavky schémy boli objektívne a systematicky overené a boli písomne dokumentované dôkazy potvrdzujúce kompetentnosť kandidáta.

Vlastník certifikačnej schémy priebežne overuje účinnosť metód na posudzovanie žiadateľov. Týmto overením sa zabezpečí, aby každé posúdenie bolo spravodlivé a platné.

Konkrétne hodnotiace kritériá a metódy, ktoré sa majú použiť, vrátane druhov hodnotenia, s cieľom preukázať, že sa dosiahli požadované ciele, môžu byť predmetom samostatných metodických usmernení vlastníka certifikačnej schémy.

4.3 ODBORNÁ SKÚŠKA

4.3.1 Obsah odbornej skúšky

Odborná skúška audítora kybernetickej bezpečnosti sa vykonáva zo znalosti všeobecne záväzných právnych predpisov upravujúcich kybernetickú bezpečnosť a ochranu kritickej infraštruktúry v kontexte informačných a komunikačných technológií a oblastí spôsobilostí uvedených v kapitole 3.2.

Odborná skúška je vykonávaná formou testu obsahujúceho 100 otázok zo znalosti všeobecne záväzných právnych predpisov a príslušných technických noriem o podmienkach výkonu činnosti audítora kybernetickej bezpečnosti a o bezpečnostných opatreniach v kybernetickej bezpečnosti. Konkrétny rozsah otázok je riešený v nasledujúcom článku tejto schémy.

Pre každú skúšku sa vygeneruje **100 otázok** náhodným výberom zo súboru obsahujúceho najmenej **400 otázok** schválených vlastníkom certifikačnej schémy.

Návrh každej skúšobnej otázky obsahuje:

a) znenie skúšobnej otázky, alebo príkladu s jednoznačným zadaním úlohy,
b) návrh štyroch alternatívnych odpovedí pre danú otázku, z ktorých len jedna odpoveď môže byť správna,
c) označenie správnych a nesprávnych odpovedí,
d) vymedzenie odbornej domény, do ktorej príslušný návrh otázky patrí,
e) voliteľne – komentár ku spôsobu riešenia navrhnutej otázky.

Každá skúšobná otázka má rovnaké bodové ohodnotenie.

Každá otázka má 4 možnosti odpovedí, pričom správna je len jedna odpoveď. **Časový rozsah skúšky na 100 otázok je 200 minút** (t. j. 2 min./otázka).

Národný bezpečnostný úrad ako vlastník certifikačnej schémy na svojom webovom sídle zverejňuje okruhy a príklady otázok na vykonanie odbornej skúšky a usmernenie na ich používanie.

4.3.2 Požiadavky na skúšobné otázky

Každý orgán posudzovania zhody uchováva skúšobné otázky / prípadové štúdie / scenáre pre potreby odbornej skúšky. Štruktúra a obsah množiny otázok sa vzťahuje na vedomosti a zručnosti definované v platnej špecifikácii spôsobilostí.

Pre každú odbornú skúšku musí byť k dispozícii trojnásobný počet otázok vybratých pre skúšku. Otázky musia byť vyberané tak, aby sa zabezpečila nezávislosť jednotlivých skúšok.

Okruhy skúšobných otázok musia obsahovať otázky z nasledujúcich odborných domén:

a) auditné postupy
b) riadenie informačnej bezpečnosti
c) riadenie IT služieb
d) IT architektúra
e) riadenie hrozieb a rizík
f) vývoj systémov (SDLC)
g) riadenie dodávateľov
h) bezpečnosť prevádzky IT
i) riešenie incidentov
j) bezpečnosť OT/SCADA
k) personálna bezpečnosť
l) riadenie kontinuity
m) strategický manažment
n) legislatíva a štandardy

4.3.3 Príprava otázok na odbornú skúšku

Za prípravu otázok na odbornú skúšku audítora kybernetickej bezpečnosti je zodpovedný orgán posudzovania zhody.

Množina skúšobných otázok musí byť najmenej 30 dní pred ich zaradením do procesu skúšky predložená vlastníkovi certifikačnej schémy na schválenie. Vlastník certifikačnej schémy má výhradné právo na zmenu, pridanie, alebo odstránenie akejkoľvek otázky z množiny navrhnutých skúšobných otázok. Vlastník certifikačnej schémy sa ku predloženým otázkam vyjadrí najneskôr v lehote do 20 dní. Po schválení množiny otázok vlastníkom

certifikačnej schémy, môže orgán posudzovania zhody danú množinu otázok používať v procese skúšky. Orgán posudzovania zhody zabezpečí, aby sa neplatné verzie množín otázok uchovávali v archíve po dobu 3 rokov.

4.3.4 Kvalifikačné požiadavky na skúšajúcich

Skúšajúci musí spĺňať nasledujúce kvalifikačné predpoklady:

- schopnosť plynulo a zrozumiteľne komunikovať v slovenskom alebo českom jazyku,
- ovládanie procesov skúšky, jej priebehu a vyhodnotenia,
- ovládanie technických testovacích prostriedkov (pre dištančnú / online formu skúšky),
- znalosť problematiky, ktorá je predmetom skúšky,
- spoľahlivosť a nestrannosť.

4.3.5 Termín a miesto vykonania odbornej skúšky

Termín, miesto a metódu vykonania odbornej skúšky určuje orgán posudzovania zhody.

Pozvánka na odbornú skúšku sa doručuje žiadateľovi v elektronickej podobe najneskôr 15 dní pred termínom konania skúšky.

Ak sa žiadateľ na skúšku nedostaví, ale vopred sa ospravedlní, je automaticky zaradený a pozvaný na najbližší voľný termín.

V prípade, že sa žiadateľ nedostaví ani na náhradný termín odbornej skúšky, orgán posudzovania zhody môže navrhnúť vyradenie tohto žiadateľa zo zoznamu žiadateľov. Vyradenie žiadateľa podlieha schváleniu vedúcim certifikačného orgánu.

Ak kandidát nebol na skúške úspešný, môže sa po obdržaní rozhodnutia o skúške prihlásiť na ďalší voľný termín skúšky. Početnosť opakovaní skúšky nie je limitovaná.

Orgán posudzovania zhody informuje vlastníka schémy o termíne a miesta vykonania odbornej skúšky najmenej 10 dní pred termínom skúšky. Orgán posudzovania zhody umožní vlastníkovi schémy na jeho vyžiadanie, zúčastniť sa na priebehu skúšky v roly pozorovateľa.

4.3.6 Priebeh odbornej skúšky

Test sa vykonáva písomnou formou, a to buď prezenčne alebo dištančne za použitia vhodných technických prostriedkov. O spôsobe vykonania testu musia byť kandidáti informovaní v pozvánke na skúšku.

Priebeh odbornej skúšky riadi skúšajúci podľa postupu Pokyny pre skúšajúcich a metodika skúšky, ktoré obsahujú aj postup na vyhodnotenie skúšky.

Pred začatím odbornej skúšky kandidát preukáže svoju totožnosť dokladom totožnosti a orgán posudzovania zhody ho poučí o pravidlách priebehu skúšky. Ak kandidát pred začatím odbornej skúšky nepreukáže svoju totožnosť alebo sa počas skúšky správa v rozpore s pravidlami priebehu skúšky a dobrými mravmi, skúšajúci rozhodne o vylúčení kandidáta zo skúšky a hľadí sa na neho akoby skúšku vykonal neúspešne. Vylúčenie kandidáta zo skúšky musí byť skúšajúcim písomne odôvodnené.

Kandidát je po celý čas prípravy a priebehu odbornej skúšky, ktorá sa vykonáva dištančnou formou, monitorovaný použitím video konferenčných nástrojov. V prípade pokynu skúšajúceho je kandidát povinný preukázať, že v miestnosti sa nenachádza iná osoba.

4.3.7 Vyhodnotenie odbornej skúšky

Skúšajúci vyhodnotí správnosť odpovedí. V prípade písomne vykonávanej skúšky prostredníctvom pripravenej šablóny správnych odpovedí, správne odpovede vyznačí zakrúžkovaním čísla otázky.

V prípade skúšky vykonanej dištančne za použitia technických prostriedkov sú odpovede vyhodnotené pomocou reportovacej funkcie softvérového testovacieho nástroja.

Kandidát sa považuje za **úspešného**, ak v skúške dosiahne **najmenej 75%** správnych odpovedí.

Kandidát sa považuje za **neúspešného**, ak v skúške dosiahne v hodnotení **menej ako 75%** správnych odpovedí.

Dokumentácia priebehu a výsledkov odbornej skúšky, testovacie otázky, vyhodnotenia testov a štatistiky úspešnosti nie sú kandidátom sprístupňované.

Sťažnosti na priebeh skúšky alebo vyhodnotenie skúšky, vrátane odvolaní proti vyhodnoteným výsledkom sa vybavujú v zmysle postupu uvedeného v kapitole 6.

5 CERTIFIKÁT

5.1 UDELENIE CERTIFIKÁTU

Podkladmi pre vydanie certifikátu audítora kybernetickej bezpečnosti je splnenie všeobecných požiadaviek na spôsobilosť podľa tejto certifikačnej schémy **a výsledky odbornej skúšky**. Certifikát vydáva kompetentná osoba v súlade s požiadavkami na orgán posudzovania zhody podľa technickej normy[4)] a v súlade s touto certifikačnou schémou.

Platnosť certifikátu audítora kybernetickej bezpečnosti sa začína dňom vydania certifikátu audítora kybernetickej bezpečnosti, ktorý je svojim označením totožný s dňom uvedeným na rozhodnutí o udelení certifikátu audítora kybernetickej bezpečnosti. Certifikát audítora kybernetickej bezpečnosti sa doručuje elektronicky, alebo si ho môže audítora kybernetickej bezpečnosti na základe vlastnej žiadosti prevziať osobne.

Doba platnosti certifikátu audítora kybernetickej bezpečnosti je **3 roky od jeho vydania**. Audítor kybernetickej bezpečnosti počas doby platnosti certifikátu audítora kybernetickej bezpečnosti využíva svoj certifikát audítora v súlade s podmienkami a obmedzeniami v ňom uvedenými, poskytuje na vyžiadanie súčinnosť orgánu posudzovania zhody a zaväzuje sa poskytnúť mu pravdivé informácie a dokumenty vyžadované touto schémou. Svoju činnosť vykonáva audítor kybernetickej bezpečnosti odborne a v súlade s dobrými mravmi.

5.2 DOHĽAD NAD ČINNOSŤOU CERTIFIKOVANÉHO AUDÍTORA KYBERNETICKEJ BEZPEČNOSTI

Posudzovanie zhody sa môže skončiť vydaním vyhlásenia, vo forme certifikátu audítora kybernetickej bezpečnosti. V prípade osobitného zreteľa alebo osobitnej povahy je certifikačný orgán oprávnený vykonať mimoriadny dohľad, ktorého cieľom je potvrdiť alebo vyvrátiť prípadne pochybnosti o plnení stanovených touto schémou.

O vykonaní mimoriadneho dohľadu nad činnosťami vykonávanými certifikovanými audítormi kybernetickej bezpečnosti písomne rozhodne vedenie orgánu posudzovania zhody. Rozhodnutie môže byť vykonané na základe:

- vlastného rozhodnutia v prípade, že sa podmienky posúdenia objektu posudzovania zhody časom zmenili, čo by mohlo ovplyvniť pokračujúce plnenie požiadaviek tejto schémy
- žiadosti objektu posudzovania zhody, ktorý si vyžaduje ďalšie preukázanie, že požiadavky sa skutočne plnia,
- obdŕžanej sťažnosti na činnosť audítora kybernetickej bezpečnosti, alebo na základe informácie o možnom porušovaní povinností podľa tejto certifikačnej schémy.

V rámci dohľadu sa môže vykonať:

- pohovor s audítorom kybernetickej bezpečnosti s cieľom zistiť jeho znalosti a zručnosti, zvyšovanie znalostí absolvovaním kurzov a pod.,

[4)] ISO/IEC 17024:2012 Posudzovanie zhody - Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb.

- kontrola záznamov audítora kybernetickej bezpečnosti o sťažnostiach zainteresovaných strán, sťažnostiach Národného bezpečnostného úradu, ich vybavenie, nápravné opatrenia a ich účinnosť,
- zaslanie upozornení certifikovaným audítorom zo strany orgánu posudzovania zhody na prípadné porušenia alebo iné zistenia, ktoré by mohli byť v rozpore s etickým kódexom certifikovaného audítora, certifikačnými požiadavkami orgánu posudzovania zhody alebo požiadavkami certifikačnej schémy.

V odôvodnených prípadoch sa môže pri dohľade vykonať posúdenie vlastného výkonu auditu kybernetickej bezpečnosti. Na tento účel orgán posudzovania zhody využíva len vlastných zamestnancov, ktorí sú viazaní mlčanlivosťou pri danom výkone posúdenia voči posudzovanému subjektu. O vykonanom dohľade spracuje orgán posudzovania zhody zápis, ktorý okrem zistených skutočností obsahuje aj termín predloženia nápravných opatrení na odstránenie zistených nedostatkov. Zápis orgán posudzovania zhody prerokuje s certifikovaným audítorom kybernetickej bezpečnosti, ktorý svojim podpisom potvrdí oboznámenie sa s protokolom, a ak s niektorými závermi nesúhlasí, uvedie svoje stanovisko (námietky, zdôvodnenie nesúhlasu). Záznamy z dohľadov sa evidujú v spise audítora. Výkonom takéhoto posúdenia certifikovaný audítor neporušil žiadnu povinnosť mlčanlivosti.

5.3 OBNOVA CERTIFIKÁTU A PREDĹŽENIE PLATNOSTI CERTIFIKÁTU

5.3.1 Obnova platnosti certifikátu audítora

O obnovu certifikátu audítora kybernetickej bezpečnosti možno požiadať po predchádzajúcom pozastavení len pred uplynutím doby platnosti aktuálne platného certifikátu audítora:

a) ak to vyplýva zo všeobecne záväzných právnych predpisov,
b) na základe zmeny požiadaviek certifikačnej schémy,
c) vzhľadom na povahu a rozvinutosť priemyslu alebo odvetvia, v ktorom audítor pôsobí,
d) vzhľadom na prebiehajúce zmeny v technológiách a požiadavkách na audítorov alebo
e) na základe odôvodnenej požiadavky zainteresovaných strán.

Na žiadosť, konanie a na vydanie certifikátu audítora kybernetickej bezpečnosti a na certifikát audítora kybernetickej bezpečnosti sa vzťahujú ustanovenia o certifikácii audítora kybernetickej bezpečnosti a certifikačná schéma.

5.3.2 Predĺženie platnosti certifikátu audítora

Pred uplynutím doby platnosti certifikátu audítora kybernetickej bezpečnosti môže audítor kybernetickej bezpečnosti požiadať o predĺženie platnosti svojho certifikátu audítora kybernetickej bezpečnosti na ďalšie trojročné obdobie. Žiadosť sa podáva najneskôr tri mesiace pred skončením platnosti certifikátu audítora kybernetickej bezpečnosti. O výnimkách z požiadaviek na dodržanie lehôt audítormi kybernetickej bezpečnosti, rozsahu a forme poskytnutých podkladov v individuálnych prípadoch rozhoduje orgán posudzovania zhody. Uplatnenie každej výnimky musí byť písomne zdôvodnené a nesmie byť v rozpore s touto certifikačnou schémou.

Podmienkou pre vydanie nového certifikátu audítora kybernetickej bezpečnosti je, že audítor kybernetickej bezpečnosti:

a) počas doby platnosti certifikátu spĺňa podmienky ustanovené v časti 3.1. a 3.2 tejto schémy a
b) preukáže, že:
   - si udržiava vedomosti a prax: udržiavanie praktických zručností doložením výkonu praxe audítora počas doby platnosti certifikátu v rozsahu minimálne päť vykonaných auditov kybernetickej bezpečnosti počas trojročného obdobia platnosti certifikátu (orgán posudzovania zhody je oprávnený preveriť pravdivosť výkonu daných auditov, a to prostredníctvom informácií o auditovanom subjekte doložených certifikovaným audítorom: rok výkonu auditu kybernetickej bezpečnosti, názov organizácie, auditovaná oblasť, overiteľná referencia – meno/pozícia, telefónne číslo),

- si zvyšuje kvalifikáciu v oblasti kybernetickej bezpečnosti najmenej v rozsahu absolvovania 60 hodín odborného vzdelávania v informačnej a kybernetickej bezpečnosti počas doby platnosti certifikátu,
- je nezávislý a predchádza konfliktu záujmov (dokladá sa čestným prehlásením, nezávislosť a predchádzanie konfliktu záujmov musí byť dodržané počas celého obdobia platnosti certifikátu).

Zvyšovanie kvalifikácie pozostáva najmä z:

- účasti na školeniach, konferenciách a webinároch v oblasti kybernetickej bezpečnosti (doložením rozsahu podujatia v hodinách),
- samoštúdiom odbornej literatúry v rozsahu max. 15 hodín ročne (dokladuje sa čestným prehlásením a zoznamom odbornej literatúry),
- publikačnej činnosti (každá normostrana publikácie sa akceptuje ako jedna hodina),
- prednáškovej činnosti (akceptuje sa jedna hodina za každú odprednášanú hodinu, na prípravu prednášky je možné započítať päťnásobok času prednášania pri jedinečnom obsahu prednášky a jedennásobok času prednášania pri opakovanom prednášaní prednášky).

5.3.3 Zmena predmetu certifikácie

Certifikačná schéma v tejto verzii nepredpokladá zavedenie rôznych úrovní certifikácie, ani zmenu predmetu certifikácie.

5.4 POZASTAVENIE ALEBO ZRUŠENIE CERTIFIKÁTU AUDÍTORA

Pozastavenie platnosti certifikátu audítora môže nastať rozhodnutím orgánu posudzovania zhody na základe podnetu NBÚ, alebo na základe požiadania audítora kybernetickej bezpečnosti.

5.4.1 Pozastavenie alebo zrušenie platnosti certifikátu orgánom posudzovania zhody

Orgán posudzovania zhody môže pozastaviť alebo zrušiť platnosť certifikátu audítora kybernetickej bezpečnosti v nasledujúcich prípadoch:

- certifikovaná osoba nespĺňa všeobecné predpoklady na výkon činnosti audítora (bod 3.1.3 tejto schémy);
- certifikovaná osoba preukázateľne nedodržiava etický kódex;
- certifikovaný audítor kybernetickej bezpečnosti dobrovoľne požiada o pozastavenie alebo zrušenie platnosti certifikátu.

Orgán posudzovania zhody je povinný tieto okolnosti prešetriť a prijať príslušné opatrenia. Ak nedôjde v lehote určenej orgánom posudzovania zhody, ktorá nesmie byť kratšia ako 30 dní, k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu audítora kybernetickej bezpečnosti, orgán posudzovania zhody ukončí platnosť vydaného certifikátu audítora kybernetickej bezpečnosti.

Certifikačný orgán vymedzí a oznámi postup pozastavenia a zrušenia certifikátu audítora kybernetickej bezpečnosti.

5.4.2 Pozastavenie platnosti certifikátu na základe podnetu NBÚ

Orgán posudzovania zhody pozastaví platnosť certifikátu audítora kybernetickej bezpečnosti na základe podnetu Národného bezpečnostného úradu ak sa preukáže porušenie povinností podľa tejto certifikačnej schémy.

Platnosť certifikátu môže byť rozhodnutím orgánu posudzovania zhody pozastavená **na dobu najviac 90 dní**. Orgán posudzovania zhody bezodkladne písomne vyzve audítora kybernetickej bezpečnosti k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu audítora kybernetickej bezpečnosti.

Ak nedôjde v lehote určenej orgánom posudzovania zhody, ktorá nesmie byť kratšia ako 30 dní, k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu audítora, orgán posudzovania zhody zruší vydaný certifikát audítora kybernetickej bezpečnosti.

5.4.3 Pozastavenie platnosti certifikátu na základe požiadavky audítora kybernetickej bezpečnosti

Orgán posudzovania zhody pozastaví platnosť certifikátu audítora kybernetickej bezpečnosti na základe písomnej požiadavky audítora kybernetickej bezpečnosti. Takéto pozastavenie platnosti certifikátu audítora kybernetickej bezpečnosti je možné len na dobu určitú, **maximálne však na 1 rok**, z nasledujúcich dôvodov:

- zo zdravotných dôvodov, alebo
- z dôvodov hroziaceho konfliktu záujmov.

Pred uplynutím doby definovanej držiteľom certifikátu a po preverení pominutia dôvodu pozastavenia platnosti, orgán posudzovania zhody obnoví platnosť vydaného certifikátu audítora kybernetickej bezpečnosti.

5.4.4 Ukončenie platnosti certifikátu

Orgán posudzovania zhody môže ukončiť platnosť vydaného certifikátu audítora kybernetickej bezpečnosti na základe:

- písomnej požiadavky audítora kybernetickej bezpečnosti,
- nesplnenia požiadavky na nápravu skutočností, ktoré viedli k pozastaveniu platnosti certifikátu audítora kybernetickej bezpečnosti v určenej lehote.

Orgán posudzovania zhody uzatvorí s audítorom kybernetickej bezpečnosti dohodu o zdržaní sa používania všetkých odkazov na certifikovaný status audítora kybernetickej bezpečnosti, ak sa zruší platnosť certifikátu audítora kybernetickej bezpečnosti.

6 VYBAVOVANIE SŤAŽNOSTÍ

Sťažnosti na priebeh skúšky alebo vyhodnotenie skúšky, vrátane odvolaní proti vyhodnoteným výsledkom a sťažnosti na výkon činnosti audítora kybernetickej bezpečnosti spracúva a rieši orgán posudzovania zhody podľa technickej normy[4)].

Orgán posudzovania zhody je povinný na svojom webovom sídle zverejniť záväznú politiku, ktorou:

- špecifikuje postupy pre vybavovanie sťažností a odvolaní v rámci procesov certifikácie,
- špecifikuje postupy pre vybavovanie sťažností na výkon činností audítora,
- stanovuje zodpovednosti a zásady riešenia sporov.

7 VEDENIE EVIDENCIÍ

Orgán posudzovania zhody vedie evidenciu:

a) žiadostí o vydanie certifikátu audítora kybernetickej bezpečnosti,
b) dokumentácie priebehu a výsledkov odbornej skúšky,
c) dokladov preukazujúcich splnenie podmienok podľa certifikačnej schémy,
d) vydaných certifikátov audítora kybernetickej bezpečnosti,
e) iných súvisiacich dokumentov.

8 PRÍSTUP K CERTIFIKAČNEJ SCHÉME

Certifikačná schéma je verejný dokument, ktorý zverejňuje Národný bezpečnostný úrad na svojom webovom sídle.

V prípade pokrytia tejto certifikačnej schémy overenia odbornej spôsobilosti audítora kybernetickej bezpečnosti akreditáciou SNAS, vlastník certifikačnej schémy je povinný informovať SNAS o zmenách certifikačnej schémy.

Dokumenty preukazujúce akreditáciu, resp. dokumenty súvisiace s certifikačným procesom (napr. akreditáciu, záväzné politiky, vzory zmlúv, atď.) zverejňuje orgán posudzovania zhody na svojom webom sídle, v nadväznosti na zmeny certifikačnej schémy.

9 PRECHODNÉ USTANOVENIA

9.1 Overenie odbornej spôsobilosti

Orgán posudzovania zhody, ktorý je orgánom verejnej správy podľa osobitného predpisu[3], je oprávnený do 31.03.2025 vykonávať overenie odbornej spôsobilosti audítora kybernetickej bezpečnosti podľa certifikačnej schémy overenia odbornej spôsobilosti audítora kybernetickej bezpečnosti účinnej do 31.12.2024.

9.2 Akceptácia certifikátu audítora kybernetickej bezpečnosti

Všetky platné certifikáty audítora kybernetickej bezpečnosti vydané do 31.12.2024 orgánom posudzovania zhody, ktorý nie je orgánom verejnej správy podľa osobitného predpisu[3] sa do 31.05.2025 považujú za vydané v súlade s touto certifikačnou schémou overenia odbornej spôsobilosti audítora kybernetickej bezpečnosti.

9.3 Prevydanie certifikátu audítora kybernetickej bezpečnosti vydaného do 31.12.2024

Audítor kybernetickej bezpečnosti, ktorému bol vydaný certifikát audítora kybernetickej bezpečnosti do 31.12.2024 orgánom posudzovania zhody, ktorý nie je orgánom verejnej správy podľa osobitného predpisu[3], je oprávnený požiadať orgán posudzovania zhody podľa tejto schémy o prevydanie certifikátu audítora kybernetickej bezpečnosti podľa tejto schémy do 31.05.2025.

K žiadosti o prevydanie certifikátu audítora kybernetickej bezpečnosti sa prikladajú dokumenty preukazujúce splnenie požiadaviek podľa bodu 3.1.2.

Pre prevydanie certifikátu audítora kybernetickej bezpečnosti certifikačný orgán posúdi, či certifikovaný audítor kybernetickej bezpečnosti spĺňa požiadavky podľa bodu 3.1.2 a 3.1.3. Odborná skúška podľa bodu 4.3 sa nevykoná.

Prevydaný certifikát sa vydáva na dobu platnosti pôvodného certifikátu.