NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Certifikačná schéma overovania odbornej spôsobilosti audítora kybernetickej bezpečnosti

Verzia 3.5.1 zo dňa 15. októbra 2020

OBSAH

Národný bezpečnostný úrad | Budatínska 30 | 851 06 Bratislava | Slovenská republika
tel.: +421 2 6869 1111 | fax: +421 2 6869 1700 | podatelna@nbu.gov.sk | www.nbu.gov.sk

1 TERMÍNY A DEFINÍCIE

Termín	Význam
akreditácia	atestácia treťou stranou týkajúca sa orgánu posudzovania zhody, ktorá slúži ako oficiálny dôkaz kompetentnosti plniť špecifické úlohy posudzovania zhody (ISO/IEC 17000: 2004)
atestácia	vydanie osvedčenia založeného na rozhodnutí po preskúmaní, že sa preukázalo splnenie určených požiadaviek (ISO/IEC 17000: 2004)
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 (STN EN ISO/IEC 17024:2012)
audítor	orgán posudzovania zhody, ktorý je certifikovaný ako orgán príslušný na posudzovanie zhody v oblasti kybernetickej bezpečnosti.
autorizácia	zmocnenie orgánu posudzovania zhody štátom vykonávať určené činnosti posudzovania zhody (ISO/IEC 17000: 2004)
certifikačné požiadavky	súbor stanovených požiadaviek, vrátane požiadaviek schémy, ktoré je potrebné splniť, na preukázanie alebo udržanie certifikácie (STN EN ISO/IEC 17024:2012)
certifikačný orgán	orgán vykonávajúci posudzovanie zhody treťou stranou podľa certifikačnej schémy (STN EN ISO/IEC 17065: 2013)
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 (STN EN ISO/IEC 17024:2012)
certifikát	dokument vydaný certifikačným orgánom v súlade s ustanoveniami tejto medzinárodnej normy, osvedčujúci, že menovaná osoba splnila certifikačné požiadavky (STN EN ISO/IEC 17024:2012)
dohľad	systematické opakovanie činností posudzovania zhody ako základ udržania platnosti stanoviska o zhode (ISO/IEC 17000: 2004)
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 (STN EN ISO/IEC 17024:2012)
objekt posudzovania zhody	akýkoľvek konkrétny materiál, produkt, inštalácia, proces, systém, osoba alebo orgán, ktorých sa týka posudzovanie zhody (STN EN ISO/IEC 17065: 2013)
odvolanie sa	žiadosť žiadateľa, kandidáta alebo certifikovanej osoby o opätovné zváženie akéhokoľvek rozhodnutia certifikačného orgánu, ktoré sa týka ním požadovaného stavu certifikácie (STN EN ISO/IEC 17024:2012)
orgán posudzovania zhody	orgán, ktorý vykonáva služby posudzovania zhody (STN EN ISO/IEC 17024:2012)
posudzovanie	proces, ktorým sa hodnotí ako konkrétna osoba splnila požiadavky certifikačnej schémy (STN EN ISO/IEC 17024:2012)
posudzovanie zhody	dokazovanie, že sa splnili určené požiadavky týkajúce sa produktu, procesu, systému, osoby alebo orgánu (ISO/IEC 17000: 2004)
posudzovanie zhody treťou stranou	posudzovanie zhody, ktoré vykonáva osoba alebo organizácia nezávislá od osoby alebo organizácie poskytujúcej objekt, alebo od používateľských zákazníckych záujmov na objekte (STN EN ISO/IEC 17065: 2013)
skúšajúci	kompetentná osoba na vykonávanie a klasifikovanie skúšky ak skúška vyžaduje odborné hodnotenie

Termín	Význam
skúšanie (testovanie)	určenie jednej alebo viacerých charakteristík objektu 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: 2004)
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
sťažnosť	vyjadrenie nespokojnosti, inej ako v odvolaní, predložené certifikačnému orgánu jednotlivcom alebo organizáciou, vo veci činností tohto orgánu alebo certifikovanej osoby, s očakávaním odpovede (STN EN ISO/IEC 17024:2012)
vlastník schémy	organizácia zodpovedná za rozvoj a udržiavanie certifikačnej schémy (STN EN ISO/IEC 17024:2012)
žiadateľ	osoba, ktorá podala žiadosť o prijatie do certifikačného procesu (STN EN ISO/IEC 17024:2012)

2 ÚVOD

2.1 ROZSAH CERTIFIKÁCIE

Predmet certifikácie	Audítor kybernetickej bezpečnosti podľa osobitného predpisu[1)]
Opis práce a úloh	Preverenie účinnosti prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených Zákonom a vykonávacími predpismi vykonaním auditu kybernetickej bezpečnosti.

2.2 PRÁVNY ZÁKLAD A NORMATÍVNE KRITÉRIÁ

Táto certifikačná schéma sa opiera najmä o nasledovné právne úpravy a technické normy:

- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti (ďalej len „Zákon“)
- Vyhláška NBÚ č. 436/2019 Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora
- Vyhláška NBÚ č. 362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Zákon č. 56/2018 Z.z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu
- STN EN ISO/IEC 17024:2012 Posudzovanie zhody - Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb

2.3 CERTIFIKAČNÉ ROLE

2.3.1 Vlastník certifikačnej schémy

Certifikačnú schému overovania odbornej spôsobilosti audítora vydáva **Národný bezpečnostný úrad**, ako orgán dohľadu v oblasti kybernetickej bezpečnosti. Certifikačná schéma poskytuje postup pri certifikácii audítora kybernetickej bezpečnosti podľa osobitného predpisu[1)].

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**

[1)] § 29 ods. 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a vyhlášky č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora

zhody podľa tejto certifikačnej schémy a podľa odporúčaní medzinárodne akceptovaných štandardov alebo iných vecne obdobných postupov[3]) príslušným na certifikáciu personálu.

Orgán posudzovania zhody je oprávnený vydávať certifikát audítora kybernetickej bezpečnosti podľa osobitného predpisu[1)]

2.3.3 Akreditačný orgán

Vnútroštátny **akreditačný orgán** je jediný orgán v členskom štáte EÚ, ktorý vykonáva akreditáciu na základe právomoci, ktorú mu udelil štát. V Slovenskej republike je vnútroštátnym akreditačným orgánom Slovenská národná akreditačná služba (SNAS). Postavenie SNAS a jej pôsobnosť určuje zákon č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov.

Orgán posudzovania zhody je oprávnený vydávať certifikát audítora kybernetickej bezpečnosti podľa osobitného predpisu[1], len za predpokladu, že je na to akreditovaný Slovenskou národnou akreditačnou službou[2]) pre oblasť certifikácie audítorov v súlade s touto certifikačnou schémou.

3 KRITÉRIÁ CERTIFIKÁCIE

3.1 VŠEOBECNÉ POŽIADAVKY NA SPÔSOBILOSŤ

3.1.1 Minimálne všeobecné požiadavky na spôsobilosť

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 a úplné stredné odborné vzdelanie (doklad o získanom stupni vzdelania a o získanej kvalifikácii)	• skúsenosti v oblasti informačných technológií, kybernetickej bezpečnosti - najmenej **10 rokov pra**xe (životopis s uvedením kontaktu na overiteľnú referenciu, zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu), • skúsenosti v oblasti auditu informačných systémov - najmenej **7 rokov praxe** (medzinárodný certifikát z oblasti auditu informačných systémov, zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu)
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), • skúsenosti v oblasti auditu informačných systémov - najmenej **5 rokov praxe** (medzinárodný certifikát z oblasti auditu informačných systémov, zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu)
Vysokoškolské vzdelanie druhého 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), • skúsenosti v oblasti auditu informačných systémov - najmenej **3 roky praxe** (medzinárodný certifikát z oblasti auditu informačných systémov, zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu)

[2]) § 9 zákona č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

3.1.2 Požadované vedomosti

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

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** (absencia uznaných sťažností na objektívnosť počas vykonávanej praxe),
- **bezúhonnosť** (dokladá sa výpis z registra trestov nie starší ako 3 mesiace).

3.1.4 Kódex správania audítora

Audítor je povinný zdržať sa takého konania, ktoré by bolo v rozpore s požiadavkami kódexu správania audítorov. Vzhľadom na to je podmienkou vydania certifikátu, aby kandidát podpísal vyhlásenie o nestrannosti a zachovaní mlčanlivosti.

[3]) STN EN ISO/IEC 27001

3.2 OSOBITNÉ POŽIADAVKY NA SPÔSOBILOSŤ

Od kandidáta sa vyžadujú nasledujúce minimálne požiadavky (znalosti, schopnosti a predpoklady) 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,
    - 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 doplnení niektorých zákonov,
    - 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. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
    - vyhlášky NBÚ č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
    - vyhlášky NBÚ č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
    - vyhlášky NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,
    - zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o doplnení niektorých zákonov,
    - zákona č. 45/2011 Z. z. o kritickej infraštruktúre,
    - 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),
    - medzinárodných noriem rady STN EN ISO/IEC 27000 „Informačné technológie - Bezpečnostné metódy - Systémy riadenia informačnej bezpečnosti“,
    - medzinárodných noriem rady 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. Schopnosť navrhovať a uplatniť bezpečnostné stratégie a politiky.
12. Znalosť procesov a metodík riadenia rizík.
13. Znalosť postupov analýzy rizík.
14. Znalosť typických hrozieb a postupov pre identifikáciu hrozieb a zraniteľností.
15. Znalosť bezpečnostných mechanizmov.
16. Znalosť metodík podnikovej architektúry.

17. Znalosť procesov riešenia kybernetických bezpečnostných incidentov.
18. Znalosť princípov plánovania havarijnej obnovy prevádzky.
19. Znalosť procesov riadenia kontinuity činností a princípov plánovania havarijnej obnovy.
20. Znalosť princípov logovania a bezpečnostného monitorovania.
21. Znalosť zásad riadenia fyzickej a objektovej bezpečnosti.
22. Znalosť bezpečnostných mechanizmov vo fyzickej a objektovej bezpečnosti.
23. Znalosť princípov riadenia služieb v oblasti informačných technológií .
24. Znalosť princípov riadenia nákladov a rozpočtových pravidiel.
25. Schopnosť prioritizácie úloh a efektívneho priraďovania zdrojov.
26. Znalosť princípov riadenia ľudských zdrojov.
27. Znalosť konceptov počítačových sietí.
28. Znalosť zásad riadenia projektov.
29. Znalosť zásad riadenia dodávateľských služieb.
30. Znalosť zásad navrhovania a vývoja aplikácií a informačných systémov.
31. Znalosť zásad obstarávania informačných systémov.
32. Znalosť zásad aplikačnej bezpečnosti.
33. Znalosť princípov a procesov auditovania.
34. Technické vedomosti o auditovaných systémoch.
35. Znalosť metód posudzovania rizík dostatočná pre vyhodnotenie rizík auditu a posúdenia hodnotenia rizík, kategorizácie informačných systémov prevádzkovateľov.
36. Znalosť požiadaviek zákona a príslušných vyhlášok.
37. Schopnosť posúdiť dôkazy.
38. Schopnosť analyzovať riziká.
39. Schopnosť spracovať úplnú a prehľadnú záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti.
40. Schopnosť analyzovať a hodnotiť bezpečnostné mechanizmy a riešenia.

4 POSÚDENIE ZHODY

4.1 POČIATOČNÉ KRITÉRIÁ CERTIFIKÁCIE

Posúdenie spôsobilosti kandidátov podľa tejto schémy má za cieľ overiť a potvrdiť, že boli dosiahnuté požiadavky na kvalifikáciu audítora podľa Vyhlášky NBÚ č. 436/2019 Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora 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:

- na základe akceptovaných kritérií hodnotenia kybernetickej bezpečnosti,
- použitím akceptovaných metód hodnotenia kybernetickej bezpečnosti,
- 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 potvrdená atestácia splnenia všetkých týchto podmienok, sa na účely tejto schémy nazývajú „certifikáty“.

4.2 METÓDY POSUDZOVANIA

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

Typickou metódou posudzovania je:

- pozorovanie činností a stavu bezpečnostných opatrení,
- analýza predložených záznamov,

- analýza predložených postupov, predpisov a dokumentov,
- rozhovory a dotazníky

Vlastník certifikačnej schémy priebežne overuje účinnosť metód na posudzovanie kandidátov. 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 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 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) návrh bodového ohodnotenia otázky
f) voliteľne – komentár ku spôsobu riešenia navrhnutej otázky

Každá otázka má 4 možností odpovedí, pričom správna je len jedna odpoveď. **Časový rozsah skúšky na 100 otázok je 150 minút** (t.j. 1,5 min./otázka).

Národný bezpečnostný úrad ako vlastník certifikačnej schémy na svojom webovom sídle zverejňuje:

g) okruhy a príklady otázok na vykonanie odbornej skúšky a usmernenie na ich používanie,
h) vzor žiadosti o vykonanie odbornej skúšky a
i) vzor certifikátu audítora.

4.3.2 Príprava otázok na odbornú skúšku

Za prípravu otázok pre odbornú skúšku audítora je zodpovedný orgán posudzovania zhody.

Množina skúšobných otázok musí byť najmenej 14 dní pred konaním 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 10 dní.

Okruhy skúšobných otázok musí 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 Termín a miesto vykonania odbornej skúšky

Termín a miesto vykonania odbornej skúšky určuje orgán posudzovania zhody.

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

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

V prípade, že sa žiadateľ nedostaví ani na náhradný termín odbornej skúšky, orgán posudzovania zhody ho vyradí zo zoznamu žiadateľov.

4.3.4 Priebeh odbornej skúšky

Test môže byť vykonaný písomnou formou, alebo elektronickou formou použitím vhodných technických prostriedkov. O spôsobe vykonanie testu musia byť kandidáti informovaní v pozvánke na skúšku.

Priebeh odbornej skúšky riadi vedúci skúšania podľa postupu Pokyny pre skúšajúcich a metodiky skúšania, ktoré obsahujú aj postup na vyhodnotenie skúšky.

Pred začatím odbornej skúšky žiadateľ preukáže svoju totožnosť dokladom totožnosti a orgán posudzovania zhody ho poučí o pravidlách priebehu skúšky. Ak žiadateľ pred začatím odbornej skúšky nepreukáže svoju totožnosť alebo sa počas skúšky správa v rozpore s pravidlami priebehu skúšky a dobrými mravmi, vylúči sa zo skúšky a hľadí sa na neho akoby skúšku vykonal neúspešne.

Odborná skúška vykonávaná elektronicky musí byť po celý čas prípravy a priebehu skúšky monitorovaná použitím videokonferenčných nástrojov.

Skúšajúci vyhodnotí správnosť/nesprávnosť odpovedí. V prípade písomne vykonávanej skúšky prostredníctvom pripravenej šablóny správnych odpovedí, v prípade elektronicky vykonávanej skúšky pomocou reportovacej funkcie softvérového testovacieho nástroja. Správne odpovede vyznačí zakrúžkovaním čísla otázky.

Skúška sa považuje za **úspešnú**, ak kandidát dosiahne **najmenej 70%** správnych odpovedí.

Skúška sa považuje za **neúspešnú** ak kandidát dosiahne v hodnotení **menej ako 70%** správnych odpovedí.

5 CERTIFIKÁT

5.1 ROZHODNUTIE O UDELENÍ CERTIFIKÁTU

Podkladom na vydanie alebo nevydanie certifikátu audítora sú **informácie o žiadateľovi a výsledky odbornej skúšky**. Rozhodovanie o tom je nezávislé a nestranné a prijíma ho kompetentná osoba v súlade s požiadavkami na orgán posudzovania zhody podľa technickej normy[4)] a v súlade s touto certifikačnou schémou.

Platnosť certifikátu audítora sa začína dňom vydania certifikátu audítora. Certifikát audítora sa zasiela žiadateľovi elektronicky a poštou, alebo si ho môže na základe vlastnej žiadosti prevziať osobne.

[4] STN EN ISO/IEC 17024

Doba platnosti certifikátu je **3 roky od jeho vydania**. Audítor počas doby platnosti certifikátu audítora 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 odborne a v súlade s dobrými mravmi.

5.2 DOHĽAD NAD ČINNOSŤOU CERTIFIKOVANÉHO AUDÍTORA

Posudzovanie zhody sa môže skončiť udelením atestácie, vo forme certifikátu audítora kybernetickej bezpečnosti. V niektorých prípadoch sa však z dôvodov udržania platnosti stanoviska vyjadreného atestáciou môže vyžadovať opakovanie funkcií atestácie. Opakovanie funkcie atestácie sa vykonáva formou mimoriadneho dohľadu.

O vykonaní mimoriadneho dohľadu nad činnosťami vykonávanými certifikovanými audítormi kybernetickej bezpečnosti rozhodne bezodkladne riaditeľ certifikačného orgánu. 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 na zhodu,
- žiadosti objektu posudzovania zhody, ktorý si vyžaduje ďalšie preukázanie, že požiadavky sa skutočne plnia,
- obdržanej sťažnosti na činnosť audítora, alebo na základe informácie o možnom porušovaní povinností podľa tejto certifikačnej schémy.

Činnosti vykonávané pri dohľade sa plánujú s cieľom zabezpečiť potrebu udržať platnosť existujúceho stanoviska vydaného pri atestácii.

V rámci dohľadu sa môže vykonať:

- pohovor s audítorom s cieľom zistiť jeho znalosti a zručnosti v uplatňovaní postupov pri vykonávaní auditu kybernetickej bezpečnosti, zvyšovanie znalostí absolvovaním kurzov a pod.,
- kontrola vydávaných dokumentov audítora ,
- kontrola záznamov audítora o sťažnostiach zákazníkov, sťažnostiach Národného bezpečnostného úradu, ich vybavenie, nápravné opatrenia a ich účinnosť.

Ak je to potrebné, môže sa pri dohľade vykonať posúdenie vlastného výkonu auditu. Na tento účel orgán posudzovania zhody využíva len vlastných zamestnancov. O vykonanom dohľade spracuje orgán posudzovania zhody zápis, ktorý okrem zistených skutočností obsahuje aj termín predloženia nápravných opatrení na odstránenie zistených nedostatkov. Zápis prerokuje s audítorom, 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.

5.3 OBNOVA CERTIFIKÁTU A PREDĹŽENIE PLATNOSTI CERTIFIKÁTU

5.3.1 Obnova platnosti certifikátu audítora

O obnovu certifikátu audítora možno požiadať aj 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 a na certifikát audítora sa vzťahujú ustanovenia o certifikácii audítora a certifikačná schéma.

5.3.2 Predĺženie platnosti certifikátu audítora

Pred uplynutím doby platnosti certifikátu audítora môže audítor požiadať o predĺženie platnosti svojho certifikátu audítora na ďalšie trojročné obdobie. Žiadosť sa podáva najneskôr tri mesiace pred skončením platnosti certifikátu audítora.

Podmienkou pre vydanie nového certifikátu audítora je, že audítor:

a) počas doby platnosti certifikátu spĺňa podmienky certifikácie a

b) preukáže, že:

- si udržiava vedomosti a prax (udržiavanie praktických zručností doložením výkonu praxe audítora počas doby platnosti certifikátu),
- si zvyšuje kvalifikáciu v oblasti kybernetickej bezpečnosti najmenej v rozsahu absolvovania 120 hodín vzdelávania počas doby platnosti certifikátu,
- má znalosti auditovania v oblasti informačných systémov (dokladá sa platný certifikát na výkon auditu informačných systémov),
- je nezávislý a predchádza konfliktu záujmov (dokladá sa prehlásením) a
- dokladá nadobudnuté znalosti v oblasti kybernetickej bezpečnosti (dokladá sa praxou, vzdelávaním, auditmi).

Zvyšovanie kvalifikácie pozostáva napríklad z:

- účasti na školeniach v oblasti kybernetickej bezpečnosti (doložením rozsahu školenia v hodinách),
- publikačnej činnosti (akceptuje sa jedna hodina za každú normostranu publikácie),
- prednáškovej činnosti (akceptuje sa jedna hodina za každú odprednášanú hodinu, na prípravu prednášky je možné započítať trojnásobok času prednášania pri jedinečnom obsahu prednášky a jedennásobok času prednášania pri opakovanom prednášaní prednášky).

Na žiadosť, konanie a na vydanie certifikátu audítora a na certifikát audítora sa vzťahujú ustanovenia o certifikácii audítora a certifikačná schéma okrem ustanovení o odbornej skúške.

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, alebo na základe požiadania audítora.

5.4.1 Pozastavenie platnosti certifikátu na základe podnetu NBÚ

Orgán posudzovania zhody pozastaví platnosť certifikátu audítora na základe podnetu Národného bezpečnostného úradu pri porušovaní 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 k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu audítora.

Ak nedôjde v lehote určenej certifikačným orgánom k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu audítora, certifikačný orgán ukončí platnosť vydaného certifikátu audítora.

5.4.2 Pozastavenie platnosti certifikátu na základe požiadavky audítora

Orgán posudzovania zhody pozastaví platnosť certifikátu audítora na základe na základe písomnej požiadavky audítora.

Audítor môže požiadať o pozastavenie platnosti certifikátu audítora na dobu určitú, **maximálne však na 1 rok**, z nasledujúcich dôvodov:

- dlhodobej neprítomnosti,

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

Po uplynutí audítorom definovanej doby certifikačný orgán obnoví platnosť vydaného certifikátu audítora.

5.4.3 Ukončenie platnosti certifikátu

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

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

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

5.5 VYBAVOVANIE SŤAŽNOSTÍ NA VÝKON ČINNOSTI AUDÍTORA

Sťažnosti na výkon činnosti audítora spracúva a rieši orgán posudzovania zhody podľa technickej normy. [3]) v zmysle platnej politiky.

6 VEDENIE EVIDENCIÍ

Orgán posudzovania zhody vedie evidenciu:

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

7 PRÍSTUP K CERTIFIKAČNEJ SCHÉME

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

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.