



## PRÍKLADY OTÁZOK SKÚŠKY – ŠIFROVÁ OCHRANA INFORMÁCIÍ

1. Čo sa rozumie pod pojmom „systém šifrovej ochrany informácií“?
2. Čo sa rozumie pod pojmom „prostriedok šifrovej ochrany informácií“?
3. Aké sú oprávnenia zamestnancov ústredného šifrového orgánu v súvislosti s vykonávaním kontroly bezpečnosti systémov a prostriedkov šifrovej ochrany informácií?
4. Čo môže ústredný šifrový orgán vykonať, ak sa zistia závažné nedostatky na úseku šifrovej ochrany informácií v súvislosti s prevádzkou systému alebo prostriedku šifrovej ochrany informácií?
5. Aký účinok má podanie rozkladu (podľa § 61 zákona č. 71/1967 Zb. o správnom konaní (správny poriadok)) proti rozhodnutiu o zastavení prevádzky systému alebo prostriedku šifrovej ochrany informácií?
6. Za akých podmienok možno obnoviť prevádzku systému alebo prostriedku šifrovej ochrany informácií po jej zastavení ústredným šifrovým orgánom?
7. Za akých podmienok si môže, na zabezpečenie šifrovej ochrany informácií, v pôsobnosti ústredného orgánu štátnej správy jeho vedúci zriadiť rezortný šifrový orgán ako osobitné pracovisko?
8. Komu je v podmienkach ústredného orgánu štátnej správy podriadený rezortný šifrový orgán?
9. Kto určuje rozsah povinností rezortného šifrového orgánu a šifrového orgánu postaveného mu na roveň?
10. Kto schvaľuje certifikované systémy a prostriedky šifrovej ochrany informácií do prevádzky?
11. Na ochranu akého stupňa utajenia vydáva vedúci ústredného orgánu štátnej správy certifikáty pre systémy a prostriedky šifrovej ochrany informácií?
12. Čo vykoná vedúci ústredného orgánu štátnej správy pri zistení nedostatkov na úseku šifrovej ochrany informácií?
13. Aké zákonné predpoklady musí spĺňať zamestnanec na úseku šifrovej ochrany informácií?
14. Kto ustanovuje zásady šifrovej ochrany informácií?
15. Čo obsahuje dokumentácia prostriedku šifrovej ochrany informácií na účely certifikácie pre jednotlivé stupne utajenia chránených utajovaných informácií?
16. Kde je obsiahnuté konštatovanie o spôsobilosti prostriedku šifrovej ochrany informácií na ochranu utajovaných informácií mimo chránených priestorov a v zahraničí?
17. Na základe čoho možno certifikované prostriedky šifrovej ochrany informácií poskytnúť cudzej moci?
18. Do koľkých dní informuje rezortný šifrový orgán Národný bezpečnostný úrad o certifikátoch vydaných vo svojej pôsobnosti?

19. Do koľkých dní od doručenia požiadavky informuje Národný bezpečnostný úrad rezortný šifrový orgán o vydaných certifikátoch?
20. Na základe čoho možno schvaľovať prostriedky do prevádzky?
21. Na základe čoho schvaľuje vedúci prostriedok do prevádzky?
22. Ako dlho sa na rezortnom šifrovom orgáne uchováva rozhodnutie o schválení prostriedku šifrovej ochrany informácií do prevádzky spolu s návrhom rezortného šifrového orgánu?
23. Aké sú podmienky schvaľovania prostriedkov získaných na ochranu zahraničných informácií?
24. Kde sa uvádza spôsob ničenia zariadení určených na šifrovú ochranu informácií a šifrových materiálov?
25. Na aký stupeň utajenia musí byť certifikovaný prostriedok šifrovej ochrany informácií používaný na ochranu informácií s rôznym stupňom utajenia?
26. Kto môže uskutočňovať prepravu prostriedku šifrovej ochrany informácií?
27. Ako často vykonáva rezortný šifrový orgán fyzickú inventarizáciu prostriedkov šifrovej ochrany informácií?
28. Na čo sa povinnosť raz ročne vykonávať fyzickú inventarizáciu prostriedkov šifrovej ochrany informácií nevzťahuje?
29. Kto vykonáva fyzickú inventarizáciu prostriedkov šifrovej ochrany informácií?
30. Čo je šifrovým materiálom ako súčasťou prostriedku?
31. Koho informuje rezortný šifrový orgán o zmenách v údajoch evidencie zamestnancov na úseku šifrovej ochrany informácií rezortného šifrového orgánu?
32. Čo musí obsahovať žiadosť vedúceho o súhlas ústredného šifrového orgánu na zriadenie rezortného šifrového orgánu?
33. Kto vedie protokol utajovaných písomností a evidenciu dokumentácie na úseku šifrovej ochrany informácií?
34. Akého zamestnanca musí mať rezortný šifrový orgán, ak spravuje prostriedky a vyrába šifrové materiály?