**Na zkoušku:**

1. Znát základní pojmy KB (co je to KB a KO, definice KB, co je to kyberprostor, co je to KII, kybernetický incident a kybernetická událost, kybernetický útok)
2. Normy a vyhlášky KB (řada norem ISO 27000, ZoKB – od kdy platí, jaké jsou jeho hlavní cíle, kde je možné zákony a vyhlášky o KB nalézt, stupně utajení, co jsou to citlivé údaje, kdo vydává prověrky, co je a co má na starosti NÚKIB).
3. ISMS (co jsou informace, co je bezpečnost informací + důvěrnost, dostupnost a integrita, co je to ISMS + jeho IT aktivum + PDCA model)
4. Bezpečnostní role v KB podle ZoKB, jejich náplň a odpovědnost, může jedna osoba zajišťovat více rolí současně, výbor pro řízení KB
5. Hrozby a rizika KB (popsat proces hodnocení rizik, jaké máme hrozby v IT - přírodního nebo lidského původu a mohou být náhodné nebo úmyslné).
6. Audit IS (proč se dělá, průběh, čas na audit, kdo ho může provádět, výsledek auditu), penetrační testování
7. Co je to digitální stopa (aktivní a pasivní), sociální inženýrství
8. Hacker a hackerské skupiny.

Otázka u zkoušky bude ze dvou podotázek (viz výše).