1. Jaké jsou cíle ochrany informační bezpečnosti?
	1. **Důvěrnost, integrita, dostupnost, autentičnost, odpovědnost**
	2. Dostupnost, respekt, proveditelnost, pravděpodobnost, prevence
	3. Detekce, zabezpečení, šifrování, systematizace, digitalizace
	4. Snížení rizika, reakce, omezení poškození, komunikace, bezpečnost
2. Jaké typy šifrování existují?
	1. **Symetrické a asymetrické**
	2. Normální a abnormální
	3. Levé a pravé šifrování
	4. Horizontální a vertikální šifrování
3. Co znamená „symetrické šifrování“?
	1. **Stejný klíč pro šifrování a dešifrování**
	2. Veřejný klíč pro šifrování a privátní klíč pro dešifrování
	3. Výměna vygenerovaného klíče relace mezi více systémy
	4. Privátní klíč pro šifrování a veřejný klíč pro dešifrování
4. Čím se zabývá IT zabezpečení?
	1. **Výhradně elektronickým zpracováním dat**
	2. Zpracováním jakýchkoli dat (elektronické, písemné, slovní)
	3. Čistě verbálními daty
	4. Pouze písemnými daty
5. Existuje absolutní bezpečnost?
	1. **Absolutní bezpečnost existuje**
	2. Absolutní bezpečnost neexistuje
	3. Záleží na tom, s kým lidé pracují
	4. Záleží na tom, s jakými daty pracují
6. Co znamenají písmena R, E a S v rovnici R = E \* S?
	1. **Risk, pravděpodobnost, výše možné ztráty**
	2. Nadbytečnost, entita, servis
	3. Risk, důsledek, bezpečnost
	4. Reakce, pravděpodobnost, systém
7. Jaké jsou úrovně napadení?
	1. **Síťová, aplikační, uživatelská**
	2. Internet, Intranet, Extranet
	3. Mobilní zařízení, televize, rádio
	4. Antény, lidé, počítače
8. Jaké jsou typy bezpečnostních opatření?
	1. **Prevence, detekce, reakce**
	2. Zabezpečení, připojení, dostupnost
	3. Zabezpečení, omezení, prevence
	4. Omezení poškození, bezpečnost, komunikace
9. Co znamená zkratka CRC?
	1. **Cyclic Redundancy Check**
	2. Cross-Role Check
	3. Control Redundancy Command
	4. Convertible Risk Control
10. Co znamená zkratka MAC?
	1. **Mandatory Access Control**
	2. Multiple Availability Control
	3. Media Authentication Control
	4. Moderate Analysis Control
11. Co znamená zkratka DAC?
	1. **Discretionary Access Control**
	2. Dictionary Access Control
	3. Discretionary Availability Command
	4. Dictionary Authenticity Command
12. Co znamená zkratka RBAC?
	1. **Role Based Access Control**
	2. Redundancy Based Access Control
	3. Replay Based Access Control
	4. Reaction Based Access Control
13. Jaké jsou kategorie pasivního útoku?
	1. **Odposlech a analýza provozu**
	2. Maskování a úprava
	3. Vložení a opakování
	4. Odmítnutí služby
14. Co je myšleno kategorií "Odmítnutí služby"?
	1. **Útočník narušuje dostupnost komunikačního vybavení.**
	2. Útočník mění komunikaci, zpožďuje, mění nebo maže vzkazy.
	3. Útočník se maskuje jako někdo jiný.
	4. Útočník zadržuje komunikační kanál.
15. Co je myšleno kategorií „Modifikace"?
	1. **Útočník mění komunikaci, zpožďuje, mění nebo maže vzkazy.**
	2. Útočník se maskuje jako někdo jiný.
	3. Útočník narušuje komunikační kanál.
	4. Útočník přidává vzkazy ke komunikaci.
16. Co je myšleno kategorií „Maskování“?
	1. **Útočník se maskuje jako někdo jiný.**
	2. Útočník narušuje komunikační kanál.
	3. Útočník přidává vzkazy do komunikace.
	4. Útočník odešle zaznamenaná data později.
17. Co je myšleno kategorií „Odposlech"?
	1. **Útočník odposlouchává komunikaci, ale aktivně nezasahuje.**
	2. Útočník analyzuje existující data
	3. Útočník se maskuje jako někdo jiný
	4. Útočník přidává vzkazy do komunikace.
18. Co je myšleno kategorií „Vložení“?
	1. **Útočník přidává vzkazy do komunikace.**
	2. Útočník se maskuje jako někdo jiný.
	3. Útočník posílá zaznamenaná data se zpožděním.
	4. Útočník narušuje komunikační kanál.
19. Co je myšleno kategorií „Replay“?
	1. **Útočník posílá zaznamenaná data se zpožděním**
	2. Útočník vkládá vzkazy do komunikace.
	3. Útočník se maskuje jako někdo jiný.
	4. Útočník mění komunikaci, zpožďuje, mění či vymazává vzkazy.
20. Která ISO norma se zabývá řízením bezpečnosti nebo bezpečností?
	1. **ISO 27000**
	2. ISO 18000
	3. ISO 36000
	4. ISO 41000