|  |
| --- |
| **«TASDIQLAYMAN»** |
| **«Kriptologiya» kafedra mudiri**  **\_\_\_\_\_\_\_\_\_\_\_ Z. Xudoykulov**  **«\_\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_2024 yil** |

**Foydalanishlarni boshqarish fanidan yakuniy nazorati savollari**

1. “So‘rov-javob” tizimini izohlang va ularga asoslangan protokollar haqida ma’lumot bering.
2. Biometrik identifikatsiya vositalari haqida ma’lumot bering.
3. Yagona kirish tizimi(Single Sign-On)ni tushuntiring va misollar keltiring.
4. Xusnixat va imzo dinamikasi, klaviaturada ishlash ritmi orqali identifikasiyalash bo‘yicha ma’lumot bering.
5. Xesh funksiya yordamida ma’lumotni butunligini ta’minlash va undagi mavjud muammolar.
6. Xavfsizlikninng asosiy tushunchalari: maxfiylik, butunlik, foydalanuvchanlik tushunchalarini izohlang.
7. Xavfsizlikning asosiy tushunchalari: risk, aktiv, zaiflik, tahdid tushunchalarini izohlang.
8. Windows OTlarda foydalanishlarni boshqarish. NTFS fayl tizimlarida foydalanish huquqlarini izohlang.
9. Windows OTlarda foydalanishlarni boshqarish. Konteyner va Xavfsizlik identifikatorlari tushunchalarini izohlang.
10. Windows OTda foydalanuvchilar va guruhlarni boshqarish. Aniq va meros qilib olingan ruxsatlar.
11. TOTP va HOTPga asoslangan tokenlar haqida ma’lumot bering.
12. Taqsimlangan ACS arxitekturasi (Bir darajali). Uning afzalligi va kamchiligini keltiring.
13. Sertifikatlar va raqamli imzo tizimlari haqida ma’lumot bering.
14. Biometrik xususiyatlarga asoslangan autentifikasiya tizimlarini izohlang.
15. Parollarga asoslangan oddiy autentifikasiyalash tizimi afzalligi va kamchiliklarini izohlang. Ushbu tizimlarga misollar keltiring.
16. Parollar xavfsizligini ta’minlash chora tadbirlarini tushuntiring.
17. Parollar xavfsizligiga qaratilgan hujumlarni tushuntiring.
18. Parollar qanday saqlanadi va taqqoslanadi? “Tuz” yordamida parolni xeshlash maqsadini tushuntiring.
19. Parolga va tokenga asoslangan autentifikasiya usulining afzallik va kamchiliklarini tushuntiring.
20. Ochiq kalitli shifrlash tizimlariga asoslangan raqamli sertifikat va uning vazifasini yoritib bering.
21. Markazlashtirilgan ACS arxitekturasi (ko‘p darajali). Uning afzalligi va kamchiliklarini yozib bering.
22. MAC (xabarlarni autentifikasiyalash kodi) asosida ma’lumot butunligini ta’minlashni va HMAC tizimlarini tushuntiring.
23. Lokal, tarmoq va global veb identifikatorlar haqida ma’lumot bering.
24. Linux OTlarida foydalanishlarni boshqarish qanday amalga oshiriladi?
25. Kuchli parollarni yaratish va ularni eslab qolish usullarini izohlang.
26. Kod terish qurilmalari, kontaktsiz o‘qib olish qurilmalari haqida ma’lumot bering.
27. Ko‘p faktorli autentifikasiya usulini muhimligini tushuntiring va ularga misollar keltiring.
28. Kerberos protokolini izohlang.
29. Internetdan foydalanish siyosatini(Promiscuous Policy,Permissive Policy, Paranoid Policy, Prudent Policy) izohlang.
30. Identifikasiya, autentifikasiya, avtorizasiya tushunchalarini misollar yordamida tushuntiring.
31. ID kartalar va shtrix kodlarni o‘qib olish qurilmalari haqida ma’lumot bering.
32. HOTP va TOTP algoritmlarini tushuntiring.
33. Foydlanishni boshqarishning DAC usulini tushuntiring.
34. Foydalanishni boshqarishni RBAC usulini tushuntiring.
35. Foydalanishni boshqarishni MAC usulini tushuntiring.
36. Foydalanishni boshqarishni ABAC usulini tushuntiring.
37. Foydalanishni boshqarish matrisasi, ACL va C-listni tushuntiring.
38. Foydalanishlarni nazoratlash tizimlari qanday tanlanadi?
39. Foydalanishlarni boshqarishni nazoratlash tizimi kontrollerlari. Avtonom va tarmoq kontrollerlar.
40. Foydalanishlarni boshqarish va nazoratlash tizimlari(СКУД)ni izohlang.
41. Foydalanishlarni boshqarish siyosati va usullarini izohlang.
42. Fizik himoyalashda foydalanishlarni boshqarishning bajaruvchi vositalari haqida ma’lumot bering.
43. Elektron raqamli imzo tizimlarini ishlashi va vazifalarini tushuntiring.
44. Dinamik va statik parollarga izoh bering.
45. Biror narsani bilishga asoslangan autentifikasiya tizimlarini izohlang.
46. Biror narsaga egalik qilishga asoslangan autentifikasiya tizimlarini izohlang.
47. Bir va ikki tomonlama autentifikasiyani misollar yordamida tushuntiring.
48. Bir martali tokenlarga asoslangan autentifikasiya tizimini izohlang
49. Bir martali parollarni shakllantirishda psevdotasodifiy sonlar generatorlarining o‘rni va axamiyati.
50. Biometrik autentifikasiya usullariga qaratilgan hujum turlarini izohlang.
51. Biba modelini tushuntiring.
52. Bell-Lapadula modelini tushuntiring.
53. Axborot xavfsizligi siyosati(AXS)ning turlari(Tashkilot, muammo va tizimga qaratilgan AXS).
54. Axborot xavfsizligi siyosatini tushuntiring.
55. Autentifikator dasturiy vositalari bo‘yicha tahliliy ma’lumot keltiring.
56. Autentifikasiya faktorlariga misollar keltiring.
57. Apparat, dasturiy va apparat – dasturiy autentifikasiya vositalari bo‘yicha tahliliy ma’lumot keltiring.
58. Identifikatsiya, autentifikatsiya, avtorizatsiya va ma’murlash tushunchalarini izohlang.
59. Xavfsizlik siyosatining zaruriyati, afzalliklari va iyerarxiyasi haqida ma’lumot keltiring.
60. Fizik xavfsizlikni nazoratlash tizimlari haqida ma’lumotlar keltiring.
61. Mobil telefon operatsion tizimlarida foydalanishni boshqarish bo‘yicha ma’lumot keltiring.
62. Lug‘at va BruteForse hujumlarini tushuntiring va ulardan himoyalanish choralarini yoritib bering.
63. Statik parollar xavfsizligini ta’minlashdagi himoyalash tamoyillarini izohlab bering.
64. Xavfsizlik, butunlik, foydalanuvchanlik, identifikatsiya va autentifikatsiya tushunchalariga izoh bering.
65. Statik parol, Mnemonika va Kitob usullariga ma’lumot yozing.
66. Tashkilotdagi elektron va qog’oz ko‘rinishidagi ma’lumotlarning xavfsizligi qanday ta’minlanadi?
67. Xavfsizlikninng asosiy tushunchalari: risk, foydalanuvchanlik, xavfsizlik, axborot himoyasi tushunchalarini izohlang.
68. Parollar va qayd yozuvni bloklash siyosatlarini izohlang.
69. Tashkilotni fizik himoyalash choralarini yoritib bering.
70. Xavfsizlikninng asosiy tushunchalari: tahdid, hujum, yelka orqali qarash hujumi, Keylogger hujumlarini izohlang.

|  |  |  |
| --- | --- | --- |
| **Kriptologiya kafedrasi katta o‘qituvchisi** |  | **Imomaliyev A.T.** |