1. **Dasturiy xavfsizlik nima?**

A) Dasturiy ta'minotning ma'lumotlarni himoya qilish va hujumlardan saqlanish imkoniyati  
B) Dasturiy ta'minotni ishlatish uchun litsenziya olish jarayoni  
C) Dasturiy ta'minotni yangilash imkoniyati  
D) Tarmoq xavfsizligini ta'minlash

1. **Dasturiy vositalar xavfsizligi qanday texnikalar orqali amalga oshiriladi?**

A) Shifrlash, autentifikatsiya, ruxsatlar.  
B) Faqat antiviruslar orqali,  
C) Faqat tarmoqni himoyalash orqali,  
D) Faqat xavfsizlik devori (firewall) orqali,

1. **Autentifikatsiya qanday amalga oshiriladi?**
2. A) Foydalanuvchining shaxsini tasdiqlash orqali  
   B) Foydalanuvchi qurilmasini tekshirish orqali  
   C) Fayllarni skanerlash orqali  
   D) Internet tarmog'ini monitoring qilish orqali
3. **Dasturiy vositalar xavfsizligini ta'minlashda kodning qanday tahlili muhim?**

A) Statik va dinamik kod tahlili  
B) Faqat statik kod tahlili  
C) Faqat dinamik kod tahlili  
D) Kodni vizual tekshirish

1. **Zararli dasturlar qanday xususiyatlarga ega?**

A) Maqsadi foydalanuvchi yoki tizimga zarar yetkazish  
B) Maqsadi tizimni tezlatish  
C) Foydalanuvchilarning ma'lumotlarini saqlash  
D) Foydalanuvchilarning ishini osonlashtirish

1. **Tarmoq xavfsizligini qanday texnikalar ta'minlaydi?**

A) Firewall, IDS, VPN.  
B) Faqat antivirus,  
C) USB portlarini bloklash,  
D) Faqat serverni himoyalash,

1. **Dasturiy ta'minotdagi zaifliklar qanday xavf tug‘dirishi mumkin?**

A) Hujumchilarning tizimga kirishiga imkon berishi  
B) Dasturiy ta'minotni tezlashtirishi  
C) Dasturiy vositalarni arzonlashtirishi  
D) Internetga kirishni cheklashi

1. **Shifrlash algoritmlari qanday vazifani bajaradi?**

A) Ma'lumotlarni o‘qilmas holatga keltiradi  
B) Ma'lumotlarni siqadi  
C) Ma'lumotlarni o‘chiradi  
D) Ma'lumotlarni tarmoq orqali uzatadi

1. **Ochiq kalitli kriptografiya qanday ishlaydi?**

A) Ikkita kalit (ochiq va yopiq) orqali ma'lumotlarni himoyalaydi  
B) Bitta kalit yordamida ma'lumotlarni shifrlaydi  
C) Ma'lumotlarni siqadi  
D) Ma'lumotlarni tarmoqqa joylashtiradi

1. **Xavfsizlik devori (Firewall) nima?**

A) Tarmoq orqali kirish-chiqishni nazorat qiluvchi dastur yoki qurilma  
B) Ma'lumotlarni siqish vositasi  
C) Dasturlarni yuklash uchun platforma  
D) Foydalanuvchilarni autentifikatsiya qilish vositasi

1. **SQL injection hujumi qanday amalga oshiriladi?**

A) Ma'lumotlar bazasiga zararli kod kiritish orqali  
B) Fayllarni o‘zgartirish orqali  
C) Tarmoqni bloklash orqali  
D) Xotirani to‘ldirish orqali

1. **Antivirus dasturi qanday vazifani bajaradi?**

A) Zararli dasturlarni aniqlash va olib tashlash  
B) Ma'lumotlarni shifrlash  
C) Internet trafigini nazorat qilish  
D) Fayllarni tezlashtirish

1. **Phishing hujumlari qanday amalga oshiriladi?**

A) Foydalanuvchilarni aldovchi saytlarga yo‘naltirish orqali  
B) Tarmoqni uzib qo‘yish orqali  
C) Zararli dasturlarni kompyuterga o‘rnatish orqali  
D) Antivirus dasturlarini o‘chirib tashlash orqali

1. **Dasturiy vositalarni yangilashning xavfsizlikka ta'siri qanday?**

A) Zaifliklarni tuzatadi va himoyani oshiradi  
B) Tizimni sekinlashtiradi  
C) Tizimni zaif qiladi  
D) Faqat vizual o‘zgarishlar kiritadi

1. **Zaxira nusxalarini yaratish nimaga xizmat qiladi?**

A) Ma'lumotlar yo‘qolganda ularni tiklash uchun  
B) Ma'lumotlarni shifrlash uchun  
C) Ma'lumotlarni tezlashtirish uchun  
D) Ma'lumotlarni o‘chirish uchun

1. **VPN qanday ishlaydi?**

A) Foydalanuvchining tarmoqdagi ma'lumotlarini shifrlab uzatadi  
B) Tarmoqni tezlashtiradi  
C) Antivirus sifatida ishlaydi  
D) Fayllarni siqadi

1. **Xavfsizlik auditlari nimani o‘z ichiga oladi?**

A) Tizimdagi xavfsizlik zaifliklarini aniqlash va hisobot berish  
B) Tizimdagi ma'lumotlarni o‘chirish  
C) Tizimdagi barcha dasturlarni yangilash  
D) Tizimni vizual tekshirish

1. **SSL/TLS nima uchun ishlatiladi?**

A) Internet orqali ma'lumotlarni xavfsiz uzatish uchun  
B) Ma'lumotlarni siqish uchun  
C) Tarmoq tezligini oshirish uchun  
D) Dasturlarni yuklab olish uchun

1. **Zararli dasturiy ta'minotlarning qaysi turi tarmoqqa tarqaladi?**

A) Qurtlar.  
B) Rootkitlar,  
C) Trojanlar,  
D) Adware dasturlar,

1. **Rootkitlar qanday zararli dasturlardir?**

A) Foydalanuvchi yoki tizim ma'lumotlarini yashirin nazorat qilish uchun  
B) Ma'lumotlarni o‘chirish uchun  
C) Kompyuterni tezlashtirish uchun  
D) Fayllarni siqish uchun

1. **Ma'lumotlarni shifrlashning asosiy maqsadi nima?**  
   A) Maxfiylikni ta'minlash.  
   B) Fayllarni ko‘paytirish,  
   C) Kompyuterni tezlashtirish,  
   D) Tarmoqni o‘chirib qo‘yish,
2. **Autentifikatsiya uchun eng keng tarqalgan usul qaysi?**  
   A) Foydalanuvchi ismi va parol  
   B) Retina skanerlash  
   C) Ovozni aniqlash  
   D) GPS ma'lumotlari
3. **Xavfsizlik devori nima uchun ishlatiladi?**  
   A) Tarmoqdagi kirish-chiqish ma'lumotlarini nazorat qilish  
   B) Ma'lumotlarni siqish uchun  
   C) Foydalanuvchilarni autentifikatsiya qilish uchun  
   D) Tizimni tezlashtirish uchun
4. **Zararli dasturlar qanday hujum qilishlari mumkin?**  
   A) Kompyuterni zararlantiruvchi dasturlar orqali  
   B) Internet tarmoqlarini tekshirish orqali  
   C) Faqat kompyuterga zarar yetkazish uchun  
   D) Fayllarni siqish uchun
5. **SSL protokoli qanday ishlaydi?**  
   A) Ma'lumotlarni xavfsiz uzatadi.  
   B) Ma'lumotlarni o‘chiradi,  
   C) Kompyuterni himoya qiladi,  
   D) Foydalanuvchilarni autentifikatsiya qiladi,
6. **Xavfsizlik zaifligi nima?**  
   A) Tizimdagi himoya darajasining pastligi  
   B) Tizimdagi fayllarni tezlashtirish  
   C) Foydalanuvchi ma'lumotlarini saqlash  
   D) Tizimni yangilash
7. **Shaxsiy kalitli kriptografiya qanday amalga oshiriladi?**  
   A) Bir kalit yordamida shifrlash va deshifrlash qilinadi  
   B) Ikki kalit yordamida ma'lumotlarni shifrlaydi  
   C) Ma'lumotlarni faqat ochadi  
   D) Fayllarni siqadi
8. **Xavfsizlik devori qanday asosiy vazifani bajaradi?**  
   A) Tarmoq orqali ma'lumotlarning o‘tishini nazorat qiladi  
   B) Foydalanuvchilarning tarmoqni tezlashtiradi  
   C) Tarmoqdagi fayllarni siqadi  
   D) Foydalanuvchi ma'lumotlarini o‘chirish
9. **Foydalanuvchi ma'lumotlarini himoya qilishning eng samarali usuli qaysi?**  
   A) Shifrlash algoritmlaridan foydalanish  
   B) Tarmoqni bloklash  
   C) Tizimni sekinlashtirish  
   D) Fayllarni siqish
10. **Ma'lumotlarni zahira qilish nimani ta'minlaydi?**  
    A) Ma'lumotlar yo‘qolganda ularni tiklash.  
    B) Fayllarni o‘chirish,  
    C) Foydalanuvchi ma'lumotlarini tezlashtirish,  
    D) Antivirusni yangilash,
11. **Trojan dasturlari qanday ishlaydi?**  
    A) Zarar yetkazuvchi dastur o‘zini foydali dastur sifatida ko‘rsatadi  
    B) Kompyuterni tezlashtirish uchun  
    C) Fayllarni siqish uchun  
    D) Internetni tezlashtirish uchun
12. **Malumotlar bazasiga hujum qilish uchun qanday texnika ishlatiladi?**  
    A) SQL injection.  
    B) Tarmoqni tezlashtirish,  
    C) Antivirusni yangilash,  
    D) Fayllarni arxivlash,
13. **AES algoritmi nima uchun ishlatiladi?**  
    A) Ma'lumotlarni shifrlash uchun  
    B) Fayllarni o‘chirish uchun  
    C) Tizimni tezlashtirish uchun  
    D) Internetni bloklash uchun
14. **Kiber xavfsizlikda eng asosiy muammo nima?**  
    A) Ma'lumotlar o‘g‘irlanishi va tizimga zarar yetkazilishi  
    B) Foydalanuvchilarni autentifikatsiya qilish  
    C) Tizimni yangilash  
    D) Fayllarni arxivlash
15. **VPN tizimi qanday maqsadga xizmat qiladi?**  
    A) Xavfsiz internetga ulanishni ta'minlash.  
    B) Tarmoqni tezlashtirish,  
    C) Foydalanuvchi ma'lumotlarini shifrlash,  
    D) Fayllarni o‘chirish,
16. **Xavfsizlik zaifliklarini qanday dasturlar aniqlaydi?**  
    A) Antivizor va IDS (Intrusion Detection System).  
    B) Faqat antivirus,  
    C) Tizimni bloklash uchun dasturlar,  
    D) Foydalanuvchilarni autentifikatsiya qilish uchun dasturlar,
17. **Ma'lumotlarni o‘g‘irlash uchun qaysi hujum turi keng qo‘llaniladi?**  
    A) Phishing.  
    B) Antivirusni yangilash,  
    C) Tizimni sekinlashtirish,  
    D) Fayllarni arxivlash,
18. **Kiber xavfsizlikda zaifliklarni qachon tuzatish kerak?**  
    A) Imkon qadar tezroq.  
    B) Faqat tizim yangilanganida,  
    C) Tizimni sekinlashtirganida,  
    D) Tizim o‘chirilganida,
19. **Shaxsiy ma'lumotlarni himoya qilishda qanday kriptografiya qo‘llaniladi?**  
    A) Asimmetrik kriptografiya  
    B) Symmetrik kriptografiya  
    C) Antivirus dasturlari  
    D) VPN texnologiyalari
20. **Kiberhujumlar qachon sodir bo‘lishi mumkin?**  
    A) Har qanday vaqtda.  
    B) Faqat antivirus o‘chirilganda,  
    C) Internetga ulanish yo‘q bo‘lganda,  
    D) Tizim yangilanganida,
21. **Symmetrik shifrlashning asosiy kamchiligi nima?**  
    A) Bir xil kalit ikkala tomon uchun ishlatiladi  
    B) Bir kalitli tizim bo‘lmagani  
    C) Juda murakkabligi  
    D) Ma'lumotlarni tez o‘chirishi
22. **Asimmetrik shifrlashning qanday afzalligi bor?**  
    A) Har bir tomonda alohida kalit ishlatiladi  
    B) Bir xil kalit ishlatiladi  
    C) Foydalanuvchilarni tezlashtiradi  
    D) Tarmoq xavfsizligini o‘chiradi
23. **Xavfsizlik uchun dasturni statik tahlil qilish nimani anglatadi?**  
    A) Dastur kodini ishga tushirishdan oldin tekshirish  
    B) Faqat ishga tushgandan keyin tekshirish  
    C) Faqat tarmoqni himoyalash  
    D) Dastur kodini o‘chirish
24. **Dinamik tahlil qanday amalga oshiriladi?**  
    A) Dastur ishga tushirilganda uning faoliyatini kuzatish  
    B) Faqat tarmoq orqali kuzatish  
    C) Antivirus dasturini o‘rnatish orqali  
    D) Dastur kodini o‘chirish orqali
25. **Fayl tizimida ma'lumotlarning himoyalanishi qanday amalga oshiriladi?**  
    A) Ma'lumotlarni shifrlash orqali.  
    B) Faqat fayllarni o‘chirish orqali,  
    C) Tizimni yangilash orqali,  
    D) Fayllarni tezlashtirish orqali,
26. **Dasturiy hujumlarning oldini olishda qanday vosita muhim hisoblanadi?**  
    A) Antivirus dasturlari  
    B) Fayllarni o‘chirish  
    C) Diskni formatlash  
    D) Internetni uzish
27. **SQL injection hujumi qanday amalga oshiriladi?**  
    A) Ma'lumotlar bazasiga zararli SQL buyruqlar kiritish orqali  
    B) Faqat tizim fayllarini o‘zgartirish orqali  
    C) Internetdan fayllar yuklash orqali  
    D) Dasturlarni yangilash orqali
28. **Ma'lumotlar bazasini himoyalashda qaysi texnologiya qo‘llaniladi?**  
    A) Shifrlash va autentifikatsiya.  
    B) Diskni tozalash,  
    C) Faqat operativ xotirani boshqarish,  
    D) Kompyuter tezligini oshirish,
29. **Operatsion tizimning xavfsizligini ta'minlash uchun nima zarur?**  
    A) Doimiy yangilanish va xavfsizlik devori  
    B) Operatsion tizimni o‘chirish  
    C) Diskni formatlash  
    D) Dasturlarni yuklash
30. **Parollarni xavfsiz saqlash uchun qanday texnologiya qo‘llaniladi?**  
    A) Xesh funksiyalari.  
    B) Fayllarni zaxiralash,  
    C) Operatsion tizimni yangilash,  
    D) Parollarni shifrlashsiz saqlash,
31. **Xavfsizlik uchun ma'lumotlar qanday holda zahiralanadi?**  
    A) Foydalanuvchi ma'lumotlarini boshqa joyda saqlash orqali  
    B) Tizimni yangilash orqali  
    C) Diskni formatlash orqali  
    D) Antivirus o‘rnatish orqali
32. **DDoS hujumi qanday amalga oshiriladi?**  
    A) Tarmoqni bir vaqtning o‘zida ko‘plab so‘rovlar bilan yuklash orqali  
    B) Faqat tarmoqni o‘chirib qo‘yish orqali  
    C) Antivirus dasturlarini yangilash orqali  
    D) Foydalanuvchi ma'lumotlarini o‘chirish orqali
33. **Ma'lumotlarni himoya qilishda qanday xavfsizlik devori tizimlari ishlatiladi?**  
    A) Paketlarni filtrlaydigan xavfsizlik devorlari  
    B) Ma'lumotlarni o‘chirish tizimlari  
    C) Foydalanuvchilarni yangilash tizimlari  
    D) Fayllarni zaxiralash tizimlari
34. **Zararli dasturlar qanday tarqaladi?**  
    A) Foydalanuvchilarga zararli dastur orqali jo‘natiladi  
    B) Tarmoqni o‘chirib qo‘yish orqali  
    C) Internetni bloklash orqali  
    D) Antivirus dasturini o‘rnatish orqali
35. **Antivirus dasturlari nima uchun ishlatiladi?**  
    A) Zararli dasturlarni aniqlash va bartaraf etish uchun  
    B) Internet tarmog‘ini tezlashtirish uchun  
    C) Foydalanuvchilarni autentifikatsiya qilish uchun  
    D) Fayllarni siqish uchun
36. **Xavfsizlik tahlili qanday maqsad bilan amalga oshiriladi?**  
    A) Zaifliklarni aniqlash va ularni tuzatish uchun  
    B) Tizimni o‘chirish uchun  
    C) Foydalanuvchi parolini o‘zgartirish uchun  
    D) Fayllarni arxivlash uchun
37. **Ma'lumotlarni uzatishda qanday xavf mavjud?**  
    A) Ma'lumotlarni yo‘qotish yoki ularni o‘g‘irlash  
    B) Tarmoqni tezlashtirish  
    C) Kompyuterning xotirasini oshirish  
    D) Operatsion tizimni o‘chirish
38. **Foydalanuvchi autentifikatsiyasi qanday amalga oshiriladi?**  
    A) Foydalanuvchi ismi va parol orqali.  
    B) Fayllarni o‘chirish orqali,  
    C) Operatsion tizimni yangilash orqali,  
    D) Tarmoqni o‘chirish orqali,
39. **Fayllarni shifrlashning asosiy maqsadi nima?**  
    A) Ma'lumotlarni maxfiy saqlash  
    B) Fayllarni tezlashtirish  
    C) Tizimni sekinlashtirish  
    D) Internet tarmog‘ini o‘chirish
40. **Tarmoq xavfsizligini qanday vositalar bilan ta'minlash mumkin?**  
    A) Xavfsizlik devorlari va VPN texnologiyalari orqali  
    B) Tarmoqni o‘chirish orqali  
    C) Fayllarni zaxiralash orqali  
    D) Foydalanuvchilarni yangilash orqali
41. **Veb-sayt xavfsizligi uchun qaysi texnologiya muhim hisoblanadi?**  
    A) SSL sertifikati.  
    B) Fayllarni yuklash,  
    C) Operatsion tizimni yangilash,  
    D) Tarmoqni o‘chirish,
42. **Zararli dasturlardan himoyalanish uchun nima qilish kerak?**  
    A) Antivirus dasturlarini o‘rnatish  
    B) Fayllarni zaxiralash  
    C) Tizimni yangilash  
    D) Tarmoqni o‘chirish
43. **VPN texnologiyasi nima uchun ishlatiladi?**  
    A) Ma'lumotlarni himoyalash uchun.  
    B) Kompyuterning tezligini oshirish uchun,  
    C) Operatsion tizimni yangilash uchun,  
    D) Tarmoqni o‘chirish uchun,
44. **Ma'lumotlarni tiklashda qanday vosita qo‘llaniladi?**  
    A) Zaxira nusxalardan tiklash.  
    B) Internetni o‘chirib qo‘yish,  
    C) Fayllarni zaxiralash,  
    D) Tizimni yangilash,
45. **Veb-sayt hujumlarini qanday kamaytirish mumkin?**  
    A) Xavfsizlik devorlari o‘rnatish orqali.  
    B) Diskni formatlash orqali,  
    C) Kompyuter tezligini oshirish orqali,  
    D) Fayllarni o‘chirish orqali,
46. **Zararli dasturlar qanday tarzda aniqlanadi?**  
    A) Antivirus dasturlari yordamida  
    B) Tarmoqni o‘chirish orqali  
    C) Fayllarni o‘chirish orqali  
    D) Internetdan foydalanish orqali
47. **Ma'lumotlar bazasi hujumlarini oldini olishda nima yordam beradi?**  
    A) SQL injection himoyasi.  
    B) Fayllarni saqlash,  
    C) Kompyuter xotirasini oshirish,  
    D) Operatsion tizimni yangilash,
48. **Xaker hujumlarini oldini olishda nima zarur?**  
    A) Xavfsizlik devori o‘rnatish.  
    B) Tarmoqni o‘chirish,  
    C) Internetni uzish,  
    D) Kompyuter tizimini yangilash,
49. **Ma'lumotlar xavfsizligini ta'minlash uchun nima zarur?**  
    A) Shifrlash texnologiyalari  
    B) Fayllarni saqlash  
    C) Diskni formatlash  
    D) Internetni o‘chirish
50. **Kompyuter tizimini zaifliklardan himoya qilish uchun nima zarur?**  
    A) Doimiy yangilanish.  
    B) Diskni formatlash,  
    C) Fayllarni zaxiralash,  
    D) Tizimni o‘chirish,
51. **Foydalanuvchi ma'lumotlarini himoya qilish uchun qanday choralar ko‘riladi?**  
    A) Parollarni shifrlash.  
    B) Tarmoqni o‘chirish,  
    C) Fayllarni saqlash,  
    D) Diskni formatlash,
52. **Zararli dasturlarni bartaraf etishda qanday vosita yordam beradi?**  
    A) Antivirus dasturlari.  
    B) Operatsion tizimni yangilash,  
    C) Internet tarmog‘ini uzish,  
    D) Fayllarni zaxiralash,
53. **Xavfsizlik tahlili qanday vositalar yordamida amalga oshiriladi?**  
    A) Zaifliklarni skanerlash vositalari  
    B) Tarmoqni o‘chirish  
    C) Fayllarni saqlash  
    D) Kompyuter tizimini formatlash
54. **Foydalanuvchi autentifikatsiyasi qanday texnologiya yordamida amalga oshiriladi?**  
    A) Biometrik autentifikatsiya  
    B) Internetdan foydalanish  
    C) Fayllarni zaxiralash  
    D) Diskni formatlash
55. **Ma'lumotlarni himoya qilishda shifrlashning qanday turi muhim?**  
    A) Asimmetrik shifrlash.  
    B) Fayllarni o‘chirish,  
    C) Internet tarmog‘ini uzish,  
    D) Tizimni yangilash,
56. **Kompyuter tizimi xavfsizligini qanday choralari bilan oshirish mumkin?**  
    A) Xavfsizlik devorlari va yangilanishlar  
    B) Fayllarni zaxiralash  
    C) Diskni formatlash  
    D) Internetdan foydalanish
57. **Zararli dastur bilan ishlovchi foydalanuvchi kompyuterini qanday qilib himoya qilishi mumkin?**  
    A) Antivirus dasturini yangilab turish  
    B) Tarmoqni o‘chirish  
    C) Fayllarni zaxiralash  
    D) Kompyuter xotirasini oshirish
58. **SSL sertifikati nima uchun ishlatiladi?**  
    A) Ma'lumotlarni himoyalash uchun.  
    B) Diskni formatlash uchun,  
    C) Fayllarni o‘chirish uchun,  
    D) Operatsion tizimni yangilash uchun,
59. **Shaxsiy ma'lumotlarni himoya qilishda qanday texnologiyalar qo‘llaniladi?**  
    A) Ma'lumotlarni shifrlash va autentifikatsiya  
    B) Tarmoqni o‘chirish  
    C) Diskni formatlash  
    D) Internetdan foydalanish
60. **Kompyuter tarmog‘i xavfsizligini qanday vosita bilan ta'minlash mumkin?**  
    A) VPN texnologiyasi.  
    B) Fayllarni o‘chirish,  
    C) Kompyuter tezligini oshirish,  
    D) Diskni formatlash,
61. **Internet xavfsizligini oshirishda qanday texnologiya muhim hisoblanadi?**  
    A) Xavfsizlik devorlari.  
    B) Fayllarni zaxiralash,  
    C) Diskni formatlash,  
    D) Internet tarmog‘ini uzish,
62. **Zararli dastur tarqalishini oldini olish uchun qanday choralar ko‘riladi?**  
    A) Antivirus dasturlarini yangilash  
    B) Tizimni o‘chirish  
    C) Fayllarni o‘chirish  
    D) Internetdan foydalanish
63. **Parollarni xavfsiz saqlash uchun qanday choralar ko‘riladi?**  
    A) Parollarni shifrlash.  
    B) Diskni formatlash,  
    C) Fayllarni saqlash,  
    D) Kompyuter tizimini yangilash,
64. **Fayl tizimlarining xavfsizligini ta'minlashda qanday vositalar ishlatiladi?**  
    A) Fayllarni shifrlash.  
    B) Internet tarmog‘ini uzish,  
    C) Diskni formatlash,  
    D) Fayllarni saqlash,
65. **DDoS hujumlaridan himoyalanishda qanday choralar ko‘riladi?**  
    A) Xavfsizlik devorlari o‘rnatish.  
    B) Diskni formatlash,  
    C) Fayllarni o‘chirish,  
    D) Kompyuter tizimini yangilash,
66. **Zararli dastur tarqatilishining oldini olishda qaysi texnologiya yordam beradi?**  
    A) Antivirus dasturlarini o‘rnatish  
    B) Fayllarni zaxiralash  
    C) Kompyuter xotirasini oshirish  
    D) Tizimni formatlash
67. **Shaxsiy ma'lumotlarni himoya qilishda qaysi chora ko‘rilishi kerak?**  
    A) Ma'lumotlarni shifrlash  
    B) Diskni formatlash  
    C) Internetdan uzilish  
    D) Fayllarni saqlash
68. **Zaxira nusxalari nima uchun zarur?**  
    A) Ma'lumotlarni tiklash uchun  
    B) Fayllarni o‘chirish uchun  
    C) Diskni tozalash uchun  
    D) Internetni yangilash uchun
69. **Xavfsizlik sertifikatlari qaysi maqsadda qo‘llaniladi?**  
    A) Ma'lumotlarni shifrlash.  
    B) Diskni formatlash,  
    C) Fayllarni saqlash,  
    D) Kompyuter tezligini oshirish,
70. **Kompyuter xavfsizligini oshirishda qanday vosita qo‘llaniladi?**  
    A) Xavfsizlik devori o‘rnatish.  
    B) Tarmoqni o‘chirish,  
    C) Fayllarni o‘chirish,  
    D) Kompyuter xotirasini oshirish,
71. **Tarmoq xavfsizligini ta'minlashda qanday texnologiya ishlatiladi?**  
    A) VPN texnologiyasi.  
    B) Kompyuter xotirasini oshirish,  
    C) Diskni formatlash,  
    D) Fayllarni zaxiralash,
72. **Xaker hujumlariga qarshi qanday choralar ko‘riladi?**  
    A) Xavfsizlik devorlari o‘rnatish  
    B) Diskni formatlash  
    C) Fayllarni saqlash  
    D) Internetni o‘chirish
73. **Foydalanuvchi ma'lumotlarini saqlashda qanday texnologiyalar ishlatiladi?**  
    A) Shifrlash va autentifikatsiya  
    B) Internetdan uzilish  
    C) Fayllarni o‘chirish  
    D) Diskni formatlash
74. **Kompyuter viruslariga qarshi qanday vosita yordam beradi?**  
    A) Antivirus dasturlari.  
    B) Internetni o‘chirish,  
    C) Fayllarni zaxiralash,  
    D) Diskni formatlash,
75. **Axborot xavfsizligini ta'minlashda qanday texnologiyalar qo‘llaniladi?**  
    A) Ma'lumotlarni shifrlash.  
    B) Fayllarni o‘chirish,  
    C) Kompyuter tizimini yangilash,  
    D) Diskni tozalash,
76. **Zaxira nusxalari qachon muhim hisoblanadi?**  
    A) Ma'lumotlarni tiklashda.  
    B) Fayllarni zaxiralashda,  
    C) Diskni formatlashda,  
    D) Internetdan foydalanishda,
77. **Ma'lumotlar bazasi xavfsizligi qaysi texnologiyalar bilan ta'minlanadi?**  
    A) SQL injection himoyasi.  
    B) Internet tarmog‘ini uzish,  
    C) Fayllarni zaxiralash,  
    D) Kompyuter xotirasini oshirish,
78. **Zararli dasturlarni bartaraf etishning asosiy usuli qaysi?**  
    A) Antivirus dasturlarini o‘rnatish  
    B) Fayllarni saqlash  
    C) Diskni formatlash  
    D) Internetdan foydalanish
79. **DDoS hujumlaridan qanday qilib himoyalanish mumkin?**  
    A) Xavfsizlik devorlari o‘rnatish.  
    B) Tarmoqni o‘chirish,  
    C) Fayllarni o‘chirish,  
    D) Kompyuter tizimini yangilash,
80. **Ma'lumotlar xavfsizligini qanday qilib oshirish mumkin?**  
    A) Shifrlash texnologiyalarini qo‘llash  
    B) Fayllarni zaxiralash  
    C) Diskni formatlash  
    D) Internetdan foydalanish
81. **Fayllarni shifrlash nima uchun muhim?**  
    A) Ma'lumotlarni himoya qilish uchun.  
    B) Fayllarni zaxiralash uchun,  
    C) Diskni tozalash uchun,  
    D) Kompyuter tizimini yangilash uchun,
82. **Zararli dastur hujumlarini oldini olish uchun nima qilish kerak?**  
    A) Antivirus dasturlarini o‘rnatish  
    B) Fayllarni o‘chirish  
    C) Kompyuter xotirasini oshirish  
    D) Internet tarmog‘ini uzish
83. **Parollarni himoyalashda qaysi texnologiya qo‘llaniladi?**  
    A) Shifrlash.  
    B) Fayllarni saqlash,  
    C) Diskni formatlash,  
    D) Tarmoqni o‘chirish,
84. **Axborot xavfsizligini oshirishda qanday texnologiyalar muhim?**  
    A) Xavfsizlik devorlari va yangilanishlar  
    B) Fayllarni zaxiralash  
    C) Diskni formatlash  
    D) Internet tarmog‘ini uzish
85. **Zararli dastur bilan ishlashda qanday chora ko‘rilishi kerak?**  
    A) Antivirus dasturlarini yangilash  
    B) Fayllarni zaxiralash  
    C) Diskni formatlash  
    D) Kompyuter tizimini yangilash
86. **Internet xavfsizligini oshirishda qanday texnologiya qo‘llaniladi?**  
    A) Xavfsizlik devorlari o‘rnatish.  
    B) Diskni formatlash,  
    C) Fayllarni saqlash,  
    D) Kompyuter xotirasini oshirish,
87. **Ma'lumotlarni shifrlashning qaysi turi muhim hisoblanadi?**  
    A) Asimmetrik shifrlash  
    B) Fayllarni o‘chirish  
    C) Internetdan uzilish  
    D) Diskni formatlash
88. **Kompyuter tizimi zaifliklarini qanday vosita bilan aniqlash mumkin?**  
    A) Zaifliklarni skanerlash dasturlari  
    B) Fayllarni o‘chirish  
    C) Kompyuter tizimini yangilash  
    D) Internet tarmog‘ini uzish
89. **Parol xavfsizligini oshirish uchun qaysi texnologiya yordam beradi?**  
    A) Biometrik autentifikatsiya  
    B) Diskni formatlash  
    C) Fayllarni zaxiralash  
    D) Internet tarmog‘ini uzish
90. **Foydalanuvchi ma'lumotlarini shifrlash nima uchun muhim?**  
    A) Ma'lumotlarni himoya qilish uchun.  
    B) Fayllarni saqlash uchun,  
    C) Diskni formatlash uchun,  
    D) Kompyuter tizimini yangilash uchun,
91. **Tizim xavfsizligini oshirish uchun qanday texnologiyalar qo‘llaniladi?**  
    A) VPN va xavfsizlik devorlari  
    B) Fayllarni o‘chirish  
    C) Internetdan foydalanish  
    D) Diskni formatlash
92. **Antivirus dasturlarining asosiy vazifasi nima?**  
    A) Zararli dasturlarni aniqlash va yo‘q qilish  
    B) Fayllarni saqlash  
    C) Diskni zaxiralash  
    D) Internet tarmog‘ini uzish
93. **Zararli dasturlardan qanday himoyalanish mumkin?**  
    A) Antivirus dasturlarini yangilash  
    B) Diskni formatlash  
    C) Fayllarni o‘chirish  
    D) Internetdan uzilish
94. **Shifrlash texnologiyalarining asosiy maqsadi nima?**  
    A) Ma'lumotlarni himoya qilish.  
    B) Diskni formatlash,  
    C) Fayllarni zaxiralash,  
    D) Kompyuter tizimini yangilash,
95. **DDoS hujumlarining oldini olish uchun qaysi texnologiya ishlatiladi?**  
    A) Xavfsizlik devorlari.  
    B) Diskni zaxiralash,  
    C) Internet tarmog‘ini uzish,  
    D) Fayllarni o‘chirish,
96. **Xavfsizlik sertifikatlari nima uchun zarur?**  
    A) Ma'lumotlarni autentifikatsiya qilish uchun  
    B) Fayllarni saqlash uchun  
    C) Diskni formatlash uchun  
    D) Kompyuter tizimini yangilash uchun
97. **Tarmoq xavfsizligini ta'minlashda VPN texnologiyasi qanday yordam beradi?**  
    A) Ma'lumotlarni shifrlash orqali himoyalash  
    B) Fayllarni zaxiralash  
    C) Diskni formatlash  
    D) Internet tarmog‘ini uzish
98. **Shaxsiy ma'lumotlar xavfsizligi uchun qanday chora ko‘riladi?**  
    A) Ma'lumotlarni shifrlash va parollarni mustahkamlash  
    B) Fayllarni zaxiralash  
    C) Diskni formatlash  
    D) Kompyuter tizimini yangilash
99. **Zaxira nusxalari qachon foydali bo‘ladi?**  
    A) Ma'lumotlar yo‘qolganda ularni tiklash uchun  
    B) Fayllarni saqlashda  
    C) Diskni formatlashda  
    D) Internetdan foydalanishda
100. **Axborot xavfsizligi qanday yo‘l bilan ta'minlanadi?**  
     A) Shifrlash va autentifikatsiya yordamida  
     B) Fayllarni zaxiralash yordamida  
     C) Internet tarmog‘ini uzish yordamida  
     D) Diskni formatlash yordamida
101. **Ma'lumotlar shifrlanishi qaysi texnologiya bilan ta'minlanadi?**  
     A) Shifrlash algoritmlari yordamida  
     B) Fayllarni saqlash  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
102. **Tarmoqda uzatilayotgan ma'lumotlarni qanday qilib himoyalash mumkin?**  
     A) Ma'lumotlarni shifrlash orqali.  
     B) Diskni formatlash orqali,  
     C) Fayllarni o‘chirish orqali,  
     D) Internet tarmog‘ini uzish orqali,
103. **Kompyuter xavfsizligini oshirish uchun qanday dasturiy ta'minot kerak?**  
     A) Antivirus va xavfsizlik devorlari  
     B) Fayllarni zaxiralash  
     C) Diskni formatlash  
     D) Kompyuter xotirasini oshirish
104. **Axborot tizimlarining asosiy xavfsizlik choralari nima?**  
     A) Ma'lumotlarni shifrlash va xavfsizlik devorlari  
     B) Fayllarni o‘chirish  
     C) Diskni formatlash  
     D) Kompyuter tizimini yangilash
105. **Kompyuter viruslariga qarshi qanday chora ko‘rilishi kerak?**  
     A) Antivirus dasturlarini yangilash  
     B) Diskni formatlash  
     C) Fayllarni o‘chirish  
     D) Internet tarmog‘ini uzish
106. **Tarmoq xavfsizligini ta'minlashda qanday texnologiyalar ishlatiladi?**  
     A) VPN va xavfsizlik devorlari  
     B) Fayllarni saqlash  
     C) Diskni zaxiralash  
     D) Internet tarmog‘ini uzish
107. **Fayllarni shifrlash texnologiyasi nima uchun muhim?**  
     A) Ma'lumotlarni himoya qilish uchun  
     B) Fayllarni zaxiralash uchun  
     C) Diskni formatlash uchun  
     D) Internet tarmog‘ini uzish uchun
108. **Xavfsizlik devorlari nima uchun zarur?**  
     A) Tarmoq hujumlaridan himoya qilish uchun  
     B) Diskni formatlash uchun  
     C) Fayllarni saqlash uchun  
     D) Internetdan foydalanish uchun
109. **Kompyuter tizimi xavfsizligini oshirishda qanday chora ko‘riladi?**  
     A) Antivirus dasturlari va xavfsizlik devorlari  
     B) Fayllarni o‘chirish  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
110. **DDoS hujumlari qaysi texnologiya bilan bartaraf etiladi?**  
     A) Xavfsizlik devorlari yordamida.  
     B) Diskni formatlash yordamida,  
     C) Fayllarni o‘chirish yordamida,  
     D) Internet tarmog‘ini uzish yordamida,
111. **Axborot xavfsizligini ta'minlashda qanday texnologiyalar ishlatiladi?**  
     A) Shifrlash va autentifikatsiya texnologiyalari.  
     B) Fayllarni zaxiralash texnologiyalari,  
     C) Diskni formatlash texnologiyalari,  
     D) Kompyuter tizimini yangilash texnologiyalari,
112. **Internet tarmog‘ida uzatilayotgan ma'lumotlarni qanday qilib himoya qilish mumkin?**  
     A) Shifrlash texnologiyalari yordamida  
     B) Fayllarni saqlash orqali  
     C) Diskni formatlash orqali  
     D) Internetdan uzilish orqali
113. **Zararli dasturlardan himoyalanishda qanday texnologiyalar yordam beradi?**  
     A) Antivirus dasturlari va xavfsizlik devorlari  
     B) Fayllarni o‘chirish va saqlash  
     C) Diskni formatlash va zaxiralash  
     D) Internet tarmog‘ini uzish
114. **Kompyuter viruslariga qarshi qanday dasturiy ta'minot yordam beradi?**  
     A) Antivirus dasturlari.  
     B) Fayllarni zaxiralash dasturlari,  
     C) Diskni formatlash dasturlari,  
     D) Internet tarmog‘ini uzish dasturlari,
115. **Axborot tizimlarining xavfsizligini ta'minlashda qanday texnologiyalar qo‘llaniladi?**  
     A) Shifrlash va xavfsizlik devorlari.  
     B) Fayllarni o‘chirish va zaxiralash,  
     C) Diskni formatlash va yangilash,  
     D) Kompyuter tizimini yangilash va saqlash,
116. **Shaxsiy ma'lumotlarni himoya qilish uchun qanday texnologiyalar ishlatiladi?**  
     A) Shifrlash va parolni mustahkamlash  
     B) Fayllarni o‘chirish  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
117. **Xavfsizlik teshiklarini yopish uchun nima qilish kerak?**  
     A) Dasturlarni va tizimni yangilash  
     B) Fayllarni saqlash  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
118. **Axborot xavfsizligini ta'minlashda xavfsizlik devorlarining roli nima?**  
     A) Tarmoqni himoya qilish.  
     B) Fayllarni o‘chirish,  
     C) Diskni formatlash,  
     D) Internet tarmog‘ini uzish,
119. **Zaxira nusxalar nima uchun zarur?**  
     A) Ma'lumotlarni qayta tiklash uchun  
     B) Fayllarni o‘chirish uchun  
     C) Diskni formatlash uchun  
     D) Internetdan uzilish uchun
120. **Antivirus dasturlari qanday ishlaydi?**  
     A) Zararli dasturlarni aniqlab, ularni yo‘q qiladi  
     B) Fayllarni zaxiralaydi  
     C) Diskni formatlaydi  
     D) Internet tarmog‘ini uzadi
121. **Xavfsizlik tizimlarini sinash uchun qaysi usul qo‘llaniladi?**  
     A) Penetratsion testlash  
     B) Fayllarni saqlash  
     C) Diskni formatlash  
     D) Internetdan uzilish
122. **Tarmoq xavfsizligini qanday oshirish mumkin?**  
     A) VPN va xavfsizlik devorlari yordamida  
     B) Diskni zaxiralash orqali  
     C) Fayllarni o‘chirish orqali  
     D) Internet tarmog‘ini uzish orqali
123. **Axborot tizimlarida parolni mustahkamlash nima uchun zarur?**  
     A) Ma'lumotlarni himoya qilish uchun.  
     B) Fayllarni zaxiralash uchun,  
     C) Diskni formatlash uchun,  
     D) Kompyuter tizimini yangilash uchun,
124. **DDoS hujumlari qanday qilib aniqlanadi?**  
     A) Tarmoq trafigini tahlil qilish orqali  
     B) Fayllarni o‘chirish orqali  
     C) Diskni formatlash orqali  
     D) Internet tarmog‘ini uzish orqali
125. **Shifrlash texnologiyalari qayerda ishlatiladi?**  
     A) Ma'lumotlarni himoya qilishda  
     B) Fayllarni saqlashda  
     C) Diskni formatlashda  
     D) Internetdan foydalanishda
126. **Xavfsizlik kameralarini tarmoq orqali boshqarishda qanday texnologiyalar ishlatiladi?**  
     A) VPN va xavfsizlik devorlari  
     B) Fayllarni zaxiralash  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
127. **Parolni mustahkamlashning asosiy usullari nimalardan iborat?**  
     A) Kompleks parol yaratish va ikki faktorli autentifikatsiya  
     B) Fayllarni o‘chirish  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
128. **Shaxsiy ma'lumotlar qanday qilib himoya qilinadi?**  
     A) Shifrlash va xavfsizlik sertifikatlari yordamida  
     B) Fayllarni zaxiralash orqali  
     C) Diskni formatlash orqali  
     D) Internetdan foydalanish orqali
129. **Kompyuter tizimlarining xavfsizligi uchun qanday dasturiy ta'minot kerak?**  
     A) Antivirus va xavfsizlik devorlari  
     B) Fayllarni saqlash dasturi  
     C) Diskni formatlash dasturi  
     D) Internetdan foydalanish dasturi
130. **Axborot tizimlarini himoya qilishda qanday chora-tadbirlar qo‘llaniladi?**  
     A) Xavfsizlik devorlari va shifrlash texnologiyalari.  
     B) Fayllarni o‘chirish va zaxiralash,  
     C) Diskni formatlash va yangilash,  
     D) Kompyuter tizimini yangilash va parolni o‘zgartirish,
131. **Antivirus dasturlarini doimiy yangilab turish nima uchun zarur?**  
     A) Yangi zararli dasturlarga qarshi himoyani ta'minlash uchun  
     B) Fayllarni zaxiralash uchun  
     C) Diskni formatlash uchun  
     D) Internetdan foydalanish uchun
132. **Shifrlash texnologiyalari qanday turlarga bo‘linadi?**  
     A) Simmetrik va assimetrik shifrlash.  
     B) Fayllarni o‘chirish va zaxiralash,  
     C) Diskni formatlash va yangilash,  
     D) Internetdan foydalanish va zaxiralash,
133. **Axborot xavfsizligini buzish urinishlarini qanday aniqlash mumkin?**  
     A) Tizim loglarini tahlil qilish orqali  
     B) Fayllarni o‘chirish orqali  
     C) Diskni formatlash orqali  
     D) Internet tarmog‘ini uzish orqali
134. **Zararli dasturlardan himoyalanishda qanday dasturiy ta'minot ishlatiladi?**  
     A) Antivirus dasturlari.  
     B) Fayllarni saqlash dasturi,  
     C) Diskni formatlash dasturi,  
     D) Internetdan foydalanish dasturi,
135. **Kompyuter tizimlarini xavfsizlik nuqtayi nazaridan qanday himoya qilish mumkin?**  
     A) Antivirus va xavfsizlik devorlari yordamida  
     B) Fayllarni o‘chirish yordamida  
     C) Diskni formatlash yordamida  
     D) Internet tarmog‘ini uzish yordamida
136. **VPN texnologiyasi tarmoq xavfsizligini qanday ta'minlaydi?**  
     A) Tarmoq ma'lumotlarini shifrlash orqali  
     B) Fayllarni saqlash orqali  
     C) Diskni formatlash orqali  
     D) Internetdan uzilish orqali
137. **Xavfsizlik teshiklarini aniqlashda qanday texnikalar qo‘llaniladi?**  
     A) Penetratsion testlash va tarmoq tahlili.  
     B) Fayllarni zaxiralash va saqlash,  
     C) Diskni formatlash va yangilash,  
     D) Kompyuter tizimini yangilash va parolni o‘zgartirish,
138. **DDoS hujumlariga qarshi qanday chora ko‘riladi?**  
     A) Xavfsizlik devorlari va tarmoq monitoringi  
     B) Fayllarni saqlash va zaxiralash  
     C) Diskni formatlash va yangilash  
     D) Internet tarmog‘ini uzish va tiklash
139. **Zaxira nusxalar nima uchun muhim?**  
     A) Ma'lumotlarni tiklash uchun.  
     B) Fayllarni o‘chirish uchun,  
     C) Diskni formatlash uchun,  
     D) Internetdan foydalanish uchun,
140. **Ma'lumotlar xavfsizligini ta'minlashda qanday texnologiyalar qo‘llaniladi?**  
     A) Shifrlash va autentifikatsiya texnologiyalari.  
     B) Fayllarni o‘chirish va saqlash,  
     C) Diskni formatlash va yangilash,  
     D) Kompyuter tizimini yangilash va parolni mustahkamlash,
141. **Parolni mustahkamlash qanday himoya chorasi hisoblanadi?**  
     A) Ma'lumotlarni himoya qilishda asosiy chora  
     B) Fayllarni o‘chirish uchun  
     C) Diskni formatlash uchun  
     D) Internetdan uzilish uchun
142. **Xavfsizlik devorining asosiy vazifasi nima?**  
     A) Tarmoq hujumlaridan himoya qilish  
     B) Fayllarni saqlash  
     C) Diskni formatlash  
     D) Internetdan foydalanish
143. **Antivirus dasturlari qanday zararli dasturlarni aniqlaydi?**  
     A) Viruslar, troyanlar va boshqa zararli dasturlarni  
     B) Fayllarni zaxiralash  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
144. **Tarmoq xavfsizligini oshirish uchun qanday choralar ko‘riladi?**  
     A) Xavfsizlik devorlari va VPN  
     B) Fayllarni o‘chirish  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
145. **Dasturlarni yangilash nima uchun zarur?**  
     A) Xavfsizlik zaifliklarini yopish uchun  
     B) Fayllarni saqlash uchun  
     C) Diskni formatlash uchun  
     D) Internetdan uzilish uchun
146. **Kiberxavfsizlikni ta’minlashda qaysi usullar qo‘llaniladi?**  
     A) Shifrlash va autentifikatsiya  
     B) Fayllarni o‘chirish  
     C) Diskni formatlash  
     D) Internetdan uzilish
147. **Tizimning xavfsizligini saqlash uchun foydalanuvchi qanday choralar ko‘rishi kerak?**  
     A) Kuchli parol yaratish va dasturlarni yangilab turish  
     B) Fayllarni saqlash  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
148. **Axborot xavfsizligi tizimlari qanday turlarga bo‘linadi?**  
     A) Tarmoq xavfsizligi va ma'lumotlarni himoya qilish tizimlari  
     B) Fayllarni zaxiralash va saqlash tizimlari  
     C) Diskni formatlash tizimlari  
     D) Internetdan foydalanish tizimlari
149. **Zaxiralash strategiyalari qayerda qo‘llaniladi?**  
     A) Ma'lumotlarni tiklash uchun.  
     B) Fayllarni o‘chirish uchun,  
     C) Diskni formatlash uchun,  
     D) Internetdan foydalanish uchun,
150. **Kiberhujumlarga qarshi qanday dasturiy ta'minotlar mavjud?**  
     A) Antivirus va xavfsizlik devorlari.  
     B) Fayllarni saqlash dasturlari,  
     C) Diskni formatlash dasturlari,  
     D) Internet tarmog‘ini uzish dasturlari,
151. **VPN texnologiyasi qayerda qo‘llaniladi?**  
     A) Tarmoqda ma'lumotlarni xavfsiz uzatish uchun  
     B) Fayllarni saqlash uchun  
     C) Diskni formatlash uchun  
     D) Internetdan uzilish uchun
152. **Xavfsizlik tekshiruvlarini amalga oshirishda qaysi vositalar ishlatiladi?**  
     A) Penetratsion testlar va tizim monitoringi  
     B) Fayllarni o‘chirish va zaxiralash  
     C) Diskni formatlash va yangilash  
     D) Kompyuter tizimini yangilash
153. **Axborot xavfsizligini buzish urinishlari qanday tahlil qilinadi?**  
     A) Loglarni tekshirish orqali.  
     B) Fayllarni saqlash orqali,  
     C) Diskni formatlash orqali,  
     D) Internetdan uzilish orqali,
154. **Axborot xavfsizligida xavf-xatarlarni qanday boshqarish mumkin?**  
     A) Xavflarni baholash va xavfsizlik chora-tadbirlarini amalga oshirish orqali  
     B) Fayllarni saqlash va zaxiralash orqali  
     C) Diskni formatlash orqali  
     D) Internetdan uzilish orqali
155. **Axborot xavfsizligini ta’minlashda qaysi hujjatlar kerak bo‘ladi?**  
     A) Xavfsizlik siyosatlari va standartlar.  
     B) Fayllarni o‘chirish hujjatlari,  
     C) Diskni formatlash ma'lumotlari,  
     D) Internet tarmog‘idan foydalanish qoidalari,
156. **Xavfsizlik teshiklarini yopish uchun dasturlar qanday yangilanadi?**  
     A) Xavfsizlik yamalarini o‘rnatish orqali  
     B) Fayllarni saqlash orqali  
     C) Diskni formatlash orqali  
     D) Internetdan uzilish orqali
157. **Shaxsiy ma'lumotlarni himoya qilish qanday usullari mavjud?**  
     A) Shifrlash va parollarni mustahkamlash  
     B) Fayllarni saqlash va zaxiralash  
     C) Diskni formatlash va yangilash  
     D) Internetdan foydalanish
158. **Axborot xavfsizligini ta'minlash uchun qanday chora-tadbirlar qo‘llaniladi?**  
     A) Xavfsizlik devorlari va shifrlash texnologiyalari  
     B) Fayllarni o‘chirish va saqlash  
     C) Diskni formatlash va yangilash  
     D) Internet tarmog‘idan foydalanish
159. **Tarmoq xavfsizligi nima uchun muhim?**  
     A) Ma'lumotlar o‘g‘irlanishining oldini olish uchun  
     B) Fayllarni saqlash uchun  
     C) Diskni formatlash uchun  
     D) Internetdan uzilish uchun
160. **Antivirus dasturini yangilab turish nima uchun zarur?**  
     A) Yangi zararli dasturlardan himoya qilish uchun  
     B) Fayllarni zaxiralash uchun  
     C) Diskni formatlash uchun  
     D) Internet tarmog‘idan uzilish uchun
161. **Parolni himoya qilishning eng yaxshi usuli nima?**  
     A) Kompleks parol yaratish va ikki faktorli autentifikatsiyani qo‘llash  
     B) Fayllarni saqlash va zaxiralash  
     C) Diskni formatlash va yangilash  
     D) Internetdan foydalanish
162. **Axborot xavfsizligini ta’minlash uchun qanday dasturiy vositalar qo‘llaniladi?**  
     A) Antivirus, xavfsizlik devorlari va shifrlash texnologiyalari  
     B) Fayllarni saqlash va zaxiralash  
     C) Diskni formatlash va yangilash  
     D) Kompyuter tizimini yangilash va qayta tiklash
163. **Xavfsizlik zaifliklarini qanday aniqlash mumkin?**  
     A) Tarmoq trafigini tahlil qilish va loglarni tekshirish orqali  
     B) Fayllarni o‘chirish orqali  
     C) Diskni formatlash orqali  
     D) Internet tarmog‘ini uzish orqali
164. **Zaxira nusxalarni doimiy yaratish nima uchun zarur?**  
     A) Ma'lumotlarni yo‘qotish xavfidan saqlanish uchun  
     B) Fayllarni saqlash uchun  
     C) Diskni formatlash uchun  
     D) Internetdan foydalanish uchun
165. **Kiberxavfsizlikni ta’minlashda qanday usullar qo‘llaniladi?**  
     A) Shifrlash, xavfsizlik devorlari va autentifikatsiya  
     B) Fayllarni saqlash va zaxiralash  
     C) Diskni formatlash va yangilash  
     D) Internet tarmog‘ini uzish va tiklash
166. **Shaxsiy ma'lumotlarni o‘g‘irlanishidan himoya qilish uchun nima qilish kerak?**  
     A) Kuchli parollar yaratish va ikki faktorli autentifikatsiyani yoqish  
     B) Fayllarni o‘chirish va zaxiralash  
     C) Diskni formatlash va yangilash  
     D) Internetdan foydalanish
167. **Axborot tizimlarini himoya qilishda xavfsizlik siyosatlari qanday rol o‘ynaydi?**  
     A) Xavfsizlik choralarini belgilashda asosiy hujjat hisoblanadi  
     B) Fayllarni saqlash va zaxiralashda rol o‘ynaydi  
     C) Diskni formatlash va yangilashda rol o‘ynaydi  
     D) Internet tarmog‘idan foydalanishda qo‘llaniladi
168. **Axborot xavfsizligini buzish urinishlarini qanday oldini olish mumkin?**  
     A) Xavfsizlik tizimlarini doimiy yangilash va monitoring qilish orqali  
     B) Fayllarni o‘chirish va zaxiralash orqali  
     C) Diskni formatlash orqali  
     D) Internet tarmog‘idan uzilish orqali
169. **Kiberhujumlardan himoyalanishda qanday dasturiy ta'minot muhim hisoblanadi?**  
     A) Antivirus va xavfsizlik devorlari  
     B) Fayllarni saqlash dasturi  
     C) Diskni formatlash dasturi  
     D) Internetdan foydalanish dasturi
170. **Shifrlash texnologiyasining asosiy vazifasi nima?**  
     A) Ma'lumotlarni o‘g‘irlanishdan himoya qilish  
     B) Fayllarni o‘chirish  
     C) Diskni formatlash  
     D) Internetdan foydalanish
171. **Xavfsizlik kameralarining tarmoq orqali boshqarilishi qaysi texnologiyaga tayanadi?**  
     A) VPN va shifrlash.  
     B) Fayllarni saqlash,  
     C) Diskni formatlash,  
     D) Internet tarmog‘ini uzish,
172. **Antivirus dasturlarining samaradorligini qanday oshirish mumkin?**  
     A) Dasturiy ta'minotni yangilab turish orqali  
     B) Fayllarni o‘chirish orqali  
     C) Diskni formatlash orqali  
     D) Internet tarmog‘ini uzish orqali
173. **Shaxsiy kompyuterlarda xavfsizlikni qanday oshirish mumkin?**  
     A) Parolni kuchliroq qilish va xavfsizlik devorlarini faollashtirish orqali  
     B) Fayllarni zaxiralash orqali  
     C) Diskni formatlash orqali  
     D) Internetdan foydalanish orqali
174. **Axborot xavfsizligida autentifikatsiyaning asosiy maqsadi nima?**  
     A) Foydalanuvchini tasdiqlash  
     B) Fayllarni o‘chirish  
     C) Diskni formatlash  
     D) Internetdan foydalanish
175. **Zaxira nusxalarini yaratishning eng yaxshi usuli nima?**  
     A) Bulutli saqlash xizmatidan foydalanish  
     B) Fayllarni o‘chirish  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
176. **Kompyuter tizimlarida shifrlash qanday amallar uchun ishlatiladi?**  
     A) Ma'lumotlarni o‘g‘irlanishdan himoya qilish uchun  
     B) Fayllarni saqlash uchun  
     C) Diskni formatlash uchun  
     D) Internetdan foydalanish uchun
177. **Xavfsizlik kameralarini boshqarishda qanday xavfsizlik texnologiyalari qo‘llaniladi?**  
     A) VPN va xavfsizlik devorlari.  
     B) Fayllarni saqlash va zaxiralash,  
     C) Diskni formatlash va yangilash,  
     D) Internet tarmog‘ini uzish,
178. **Shaxsiy ma'lumotlarni himoya qilishda qanday texnologiyalar ishlatiladi?**  
     A) Shifrlash va autentifikatsiya texnologiyalari  
     B) Fayllarni o‘chirish va saqlash  
     C) Diskni formatlash va yangilash  
     D) Internetdan foydalanish va zaxiralash
179. **Kuchli parollar yaratishda qanday qoida qo‘llaniladi?**  
     A) Parol uzunligi va murakkabligini oshirish  
     B) Fayllarni o‘chirish  
     C) Diskni formatlash  
     D) Internet tarmog‘ini uzish
180. **Tizim xavfsizligi uchun qanday dasturlar muhim hisoblanadi?**  
     A) Antivirus va xavfsizlik devorlari  
     B) Fayllarni saqlash dasturi  
     C) Diskni formatlash dasturi  
     D) Internetdan foydalanish dasturi