

## 1) **Konfidensiallikni** ta'minlash bu - ?

Manba Kanallar:

@tatuda  
@tatu\_1k  
@tuit\_team  
@tuit\_1955  
@tatu\_baza  
@t4tuchik  
@Berilgan\_Vazifalar\_650\_20  
@TUIT\_studenti

a. Ruxsat etilmagan “o‘qishdan” himoyalash

b. Ruxsat etilmagan “yozishdan” himoyalash

c. Ruxsat etilmagan “bajarishdan” himoyalash

d. Ruxsat berilgan “amallarni” bajarish

## 2) **Foydalanuvchanlikni** ta'minlash bu - ?

a. Ruxsat etilmagan “bajarishdan” himoyalash

b. Ruxsat etilmagan “yozishdan” himoyalash

c. Ruxsat etilmagan “o‘qishdan” himoyalash

d. Ruxsat berilgan “amallarni” bajarish

## 3) **Butunlikni** ta'minlash bu - ?

a. Ruxsat etilmagan “yozishdan” himoyalash

b. Ruxsat etilmagan “o‘qishdan” himoyalash

c. Ruxsat etilmagan “bajarishdan” himoyalash

d. Ruxsat berilgan “amallarni” bajarish

## 4) **Hujumchi** kabi fikrlash nima uchun kerak?

a. Bo'lishi mumkin bo'lgan xavfni oldini olish uchun.

b. Kafolatlangan amallarni ta'minlash.

c. Ma'lumot, axborot va tizimdan foydalanish uchun.

d. Ma'lumotni aniq va ishonchli

## 5) Tizimli fikrlash nima uchun kerak?

a. Kafolatlangan amallarni ta'minlash.

b. Bo'lishi mumkin bo'lgan xavfni oldini olish uchun

c. Ma'lumot, axborot va tizimdan foydalanish uchun.

d. Ma'lumotni aniq va ishonchli ekanligini bilish uch

## 6 Risk bu?

a. Noaniqlikning maqsadlarga ta'siri

b. U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz

c. Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa

d. Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan  
istalmagan hodisa

## 7) Tahdid bu?

a. Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan  
istalmagan hodisa

b. Noaniqlikning maqsadlarga ta'siri

c. U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz

d. Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa

## 8) Aktiv bu?

**a. Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa**

- b. Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa
- c. Noaniqlikning maqsadlarga ta'siri
- d. U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz

**9) Zaiflik bu?**

**a. Bir yoki bir nechta tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik**

- b. Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa
- c. Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa
- d. Noaniqlikning maqsadlarga ta'siri

**10) Boshqarish vositasi bu?**

**a. Riskni o'zgartiradigan harakatlar bo'lib, boshqarish natijasi zaiflik yoki tahdidga ta'sir qiladi**

- b. Bir yoki bir nechta tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik
- c. Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa
- d. Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa

11) Har qanday **vaziyatga** biror bir hodisani yuzaga kelish **ehtimoli** qo'shilsa ....

a. Risk paydo bo'ladi.

b. Hujum paydo bo'ladi.

c. Tahdid paydo bo'ladi.

d. Aktiv paydo bo'ladi.

12) **Denial of service (DOS)** hujumi axborotni ....  
xususiyatini buzushga qaratilgan.

a. Foydalanuvchanlik

b. Butunlik

c. Konfidensiallik

d. Ishonchlilik

13) Tashkil etuvchilar xavfsizligi, **aloqa xavfsizligi**  
va **dasturiy** ta'minotlar xavfsizligidan iborat  
bo'lgan xavfsizlik sohasi bu?

a. Tizim xavfsizligi

b. Ma'lumotlar xavfsizligi

c. Inson xavfsizligi

d. Tashkilot xavfsizligi

14) **Kriptologiya** bu?

a. "Maxfiy kodlar"ni yaratish va buzish fani va sanati

b. "Maxfiy kodlar"ni yaratish fani va sanati

c. "Maxfiy kodlar"ni buzish fani va sanati

d. Axborotni himoyalash fani va sanati

15) .... **kriptotizimni** shifrlash va deshifrlash uchun sozlashda foydalaniladi.

a. Kalit

b. Ochiq matn

c. Alifbo

d. Algoritm

16) **Kriptografiya** bu?

a. "Maxfiy kodlar"ni yaratish fani va sanati

b. "Maxfiy kodlar"ni yaratish va buzish fani va sanati

c. "Maxfiy kodlar"ni buzish fani va sanati

d. Axborotni himoyalash fani va sanati

17) **Kriptotahlil** bu?

a. "Maxfiy kodlar"ni buzish fani va sanati

b. "Maxfiy kodlar"ni yaratish fani va sanati

- c. "Maxfiy kodlar"ni yaratish va buzish fani va sanati
- d. Axborotni himoyalash fani va sanati

**18) ..... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to'plami.**

**a. Alifbo**

- b. Ochiq matn
- c. Shifrmtn
- d. Kodlash

**19) Agar ochiq ma'lumot shifrlansa, natijasi .... bo'ladi.**

**a. Shifrmtn**

- b. Ochiq matn
- c. Nomalum
- d. Kod

**20) Deshifrlash jarayonida kalit va ..... kerak bo'ladi.**

**a. Shifrmtn**

- b. Ochiq matn
- c. Kodlash

d. Alifbo

**21) Ma'lumotni sakkizlik sanoq tizimidan o'n oltilik sanoq tizimiga o'tkazish bu?**

**a. Kodlash**

b. Shifrlash

c. Yashirish

d. Deshifrlash

**22) Ma'lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalanuvchi tizim bu?**

**a. Simmetrik kriptotizim**

b. Ochiq kalitli kriptotizim

c. Asimetrik kriptotizim

d. Xesh funksiyalar

**23) Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi?**

**a. Ochiq kalitli kriptotizim**

b. Simmetrik kriptotizim

c. Xesh funksiyalar

d. MAS tizimlari

24) Ma'lumotni mavjudligini yashirishni maqsad qilgan bilim sohasi bu?

a. Steganografiya

b. Kriptografiya

c. Kodlash

d. Kriptotahlil

25) Ma'lumotni foydalanuvchiga qulay tarzda taqdim qilish uchun ..... zarur.

a. Kodlash

b. Shifrlash

c. Yashirish

d. Deshifrlash

26) Ma'lumotni konfidensialligini ta'minlash uchun ..... zarur.

a. Shifrlash

b. Kodlash

c. Yashirish

d. Deshifrlash

27) Ma'lumotni mavjudligini yashirish uchun .....



**a. Steganografiyadan foydalaniladi.**

b. Kriptografiyadan foydalaniladi.

c. Kodlashdan foydalaniladi.

d. Kriptotahlildan foydalaniladi.

**28) Xesh funksiyalar bu?**

**a. Kalitsiz kriptografik funksiya**

b. Bir kalitli kriptografik funksiya

c. Ikki kalitli kriptografik funksiya

d. Ko'p kalitli kriptografik funksiya

**29) Ma'lumotni uzatishda kriptografik himoya .....**

**a. Konfidensiallik va butunlikni ta'minlaydi.**

b. Konfidensiallik va foydalanuvchanlikni ta'minlaydi.

c. Foydalanuvchanlik va butunlikni ta'minlaydi.

d. Konfidensiallik ta'minlaydi.

**30) Qadimiy davr klassik shifriga quyidagilarning qaysi biri tegishli?**

**a. Sezar shifri**

b. Kodlar kitobi

c. Enigma shifri

d. DES, AES shifri

**31) Kompyuter davriga tegishli shifrlarni aniqlang.**

**a. DES, AES shifri**

b. Sezar shifri

c. Kodlar kitobi

d. Enigma shifri

**32) Chastotalar tahlili bo'yicha quyidagilardan qaysi shifrlarni buzib bo'lmaydi.**

**a. O'rin almashtirish shifrlarini.**

b. Bir qiymatli o'rniga qo'yish shifrlarini.

c. Sezar shifrini.

d. Barcha javoblar to'g'ri.

**33) .... shifrlar blokli va oqimli turlarga ajratiladi.**

**a. Simmetrik**

b. Ochiq kalitli

c. Asimetrik

d. Klassik davr

**34) Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan shifrlash turi bu?**

**a. Oqimli shifrlar**

- b. Blokli shifrlar
- c. Ochiq kalitli shifrlar
- d. Asimetrik shifrlar

**35) Ochiq matn qismlarini takror shifrlashga asoslangan usul bu?**

**a. Blokli shifrlar**

- b. Oqimli shifrlash
- c. Ochiq kalitli shifrlar
- d. Asimetrik shifrlar

**36) A5/1 shifri qaysi turga mansub?**

**a. Oqimli shifrlar**

- a. Blokli shifrlar
- b. Ochiq kalitli shifrlar
- c. Asimetrik shifrlar

**37) Qaysi algoritmlar simmetrik blokli shifrlarga tegishli?**

**a. TEA, DES**

- b. A5/1, AES

c. Sezar, TEA

d. Vijniner, TEA

**38) Simmetrik kriptotizimlarning asosiy kamchiligi bu?**

**a. Kalitni taqsimlash zaruriyati**

b. Shifrlash jarayonining ko'p vaqt olishi

c. Kalitlarni esda saqlash murakkabligi

d. Foydalanuvchilar tomonidan maqbul ko'rilmaslgi

**39) Faqat simmetrik blokli shifrlarga xos bo'lgan atamani aniqlang?**

**a. Blok uzunligi**

b. Kalit uzunligi

c. Ochiq kalit

d. Kodlash jadvali

**40) Sezar shifrlash usuli qaysi akslantirishga asoslangan?**

**a. O'rniga qo'yishga**

b. O'rin almashtirishga

c. Ochiq kalitli shifrlashga

d. Kombinatsion akslantirishga

**41) Qaysi akslantirishda ochiq matn va shifratndagi belgilarning chastotalari o'zgarmaydi.**

**a. O'rniga qo'yishga**

b. O'rin almashtirishga

c. Bunday akslantirish mavjud emas

d. Kombinatsion akslantirishga

**42) Kerxgofs prinsipiga ko'ra kriptotizimning to'liq xavfsiz bo'lishi faqat qaysi kattalik nomalum bo'lishiga asoslanishi kerak ?**

**a. Kalit**

b. Algoritm

c. Shifratn

d. protokol

**43) Shaxsiy kriptotizimlar nima uchun xavfsiz emas deb qaraladi.**

**a. Tor doiradagi insonlar tomonidan ishlab chiqilgani va tahlil qilingani sababli**

- b. Faqat bitta kalitdan foydalanilgani sababli
- c. Bardoshli kalitlardan foydalanilmagani sababli
- d. Ikkita kalitdan foydalanilgani sababli

**44) Shifrlash va deshifrlash alohida kalitlardan foydalanuvchi kriptotizimlar bu?**

**a. Ochiq kalitli kriptotizimlar**

- b. Simmetrik kriptotizimlar
- c. Bir kalitli kriptotizimlar
- d. Xesh funksiyalar

**45) Agar simmetrik kalitning uzunligi 128 bit bo'lsa, jami bo'lishi mumkin bo'lgan kalitlar soni nechta?**

**a. 2128**

- b. 128!
- c. 1282
- d. 2127

$$2^{128}$$

**46) Quyidagi shifrlar orasidan ochiq kalitli turga mansublarini tanlang.**

**a. RSA**

b. TEA

c. A5/1

d. Sezar

**47) Simmetrik shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi.**

**a. Konfidensiallik va butunlik**

b. Konfidensiallik

c. Butunlik va foydalanuvchanlik

d. Foydalanuvchanlik va konfidensiallik

**48) Ochiq kalitli shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi.**

**a. Konfidensiallik va butunlik**

b. Konfidensiallik

c. Butunlik va foydalanuvchanlik

d. Foydalanuvchanlik va konfidensiallik

**49) Rad etishni oldini oluvchi kriptotizimni aniqlang.**

**a. Elektron raqamli imzo tizimi**

b. MAS tizimlari

c. Simmetrik shifrlash tizimlari

d. Xesh funksiyalar

**50) Katt sonni faktorlash muammosiga asoslangan ochiq kalitli algoritmi aniqlang.**

**a. RSA algoritmi**

b. El-Gamal algoritmi

c. DES

d. TEA

**51) Ochiq kalitli kriptotizimlarning asosiy kamchiligini ko'rsating?**

**a. Hisoblashda yuqori vaqt sarflanadi**

b. Kalitlarni taqsimlash muammosi mavjud

c. Ikkita kalitni saqlash muammosi mavjud

d. Foydalanish uchun noqulaylik tug'diradi

**52) Ochiq kalitli kriptotizimlarni rad etishdan himoyalashning asosiy sababi nimada?**

**a. Ikkita kalitdan foydalanilgani**

b. Matematik muammoga asoslanilgani

c. Ochiq kalitni saqlash zaruriyati mavjud emasligi

d. Shaxsiy kalitni saqlash zarurligi



**53) MAS (Xabarlarni autentifikatsiya kodlari) tizimlari nima uchun rad etishdan himoyalay olmaydi?**

**a. Yagona kalitdan foydalanilgani sababli**

b. Xesh funksiyadan foydalanilgani sababli

c. Shaxsiy kalitni sir saqlanishi sababli

d. Faqat ma'lumot butunligini ta'minlagani sababli

**54) Xesh funksiyaga tegishli bo'lmagan talabni aniqlang.**

**a. Bir tomonlama funksiya bo'lmashligi**

b. Amalga oshirishdagi yuqori tezkorlik

c. Turli kirishlar turli chiqishlarni akslantirishi

d. Kolliziyaga bardoshli bo'lishi

**55) Elektron raqamli imzoni shakllantirishda qaysi kalitdan foydalaniladi?**

**a. Shaxsiy kalitdan**

b. Ochiq kalitdan

c. Kalitdan foydalanilmaydi

d. Umumiy kalitdan

56) Ochiq kalitli shifrlashda deshifrlash qaysi kalit asosida amalga oshiriladi?

a. Shaxsiy kalit

b. Ochiq kalit

c. Kalitdan foydalanilmaydi

d. Umumiy kalit

57) Elektron raqamli imzo quyida keltirilganlarning qaysi birini ta'minlaydi?

a. Axborot butunligini va rad etishdan himoyalashni

b. Axborot konfidensialligini va rad etishdan himoyalashni

c. Axborot konfidensialligini

d. Axborot butunligini

58) Ochiq kalitli kriptotizim asosida dastlab shifrlab so'nga imzo qo'yish sxemasida qayday muammo mavjud?

a. Shifrmtnni ixtiyoriy kishi imzolab yuborishi mumkin

b. Imzoni ixtiyoriy kishi tekshirishi mumkin

c. Osonlik bilan shifrmtnni kalitsiz deshifrlashi mumkinligi

d. Muammo mavjud emas

59) Ochiq kalitli kriptotizim asosida dastlab **imzo** qo'yib so'nga **shifrlash** sxemasida qayday muammo mavjud?

a. Deshifrlanganidan so'ng imzolangan ma'lumotni ixtiyoriy kishiga yuborish mumkin.

- b. Shifratnni ixtiyoriy kishi imzolab yuborishi mumkin
- c. Imzoni ixtiyoriy kishi tekshirishi mumkin
- d. Muammo mavjud emas

60) Faqat ma'lumotni **butunligini** ta'minlovchi kriptotizimlarni aniqlang.

a. MAS (Xabarlarini autentifikatsiya kodlari) tizimlari

- b. Elektron raqamli imzo tizimlari
- c. Ochiq kalitli shifrlash tizimlari
- d. Barcha javoblar to'g'ri

61) Quyida keltirilgan qaysi **ketma-ketlik** to'g'ri manoga ega.

a. Identifikatsiya, autentifikatsiya, avtorizatsiya

- b. Autentifikatsiya, avtorizatsiya, identifikatsiya
- c. Identifikatsiya, avtorizatsiya, autentifikatsiya

d. Avtorizatsiya, identifikatsiya, autentifikatsiya

**62) Foydalanuvchini tizimga tanitish jarayoni bu?**

**a. Identifikatsiya**

b. Autentifikatsiya

c. Avtorizatsiya

d. Ro'yxatga olish

**63) Foydalanuvchini haqiqiyligini tekshirish jarayoni bu?**

**a. Autentifikatsiya**

b. Identifikatsiya

c. Avtorizatsiya

d. Ro'yxatga olish

**64) Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu?**

**a. Avtorizatsiya**

b. Autentifikatsiya

c. Identifikatsiya

d. Ro'yxatga olish

**65) Biror narsani bilishga asoslangan**

**autentifikatsiya** usulining asosiy kamchiligi?

**a. Esda saqlash zaruriyati**

- b. Birga olib yurish zaruriyati
- c. Almashtirib bo'lmalik
- d. Qalbakilashtirish mumkinligi

**66) Biror narsani bilishga asoslangan**

**autentifikatsiyaga** tegishli bo'lgan misollarni aniqlang.

**a. PIN, Parol**

- b. Token, mashinaning kaliti
- c. Yuz tasviri, barmoq izi
- d. Biometrik parametrlar

**67) Biror narsaga egalik qilishga asoslangan**

**autentifikatsiya** usulining asosiy kamchiligi?

**a. Doimo xavfsiz saqlab olib yurish zaruriyati**

- b. Doimo esda saqlash zaruriyati
- c. Qalbakilashtirish muammosi mavjudligi
- d. Almashtirib bo'lmalik

68) Esda saqlash va olib yurish zaruriyatini talab etmaydigan autentifikatsiya usuli bu?

a. Biometrik parametrlarga asoslangan usuli

b. Parolga asoslangan usul

c. Tokenga asoslangan usul

d. Ko'p faktorli autentifikatsiya usuli

69) Eng yuqori darajagi universallik darajasiga ega biometrik parametрни ko'rsating.

a. Yuz tasviri

b. Ko'z qorachig'i

c. Barmoq izi

d. Qo'l shakli

70) Eng yuqori darajagi takrorlanmaslik darajasiga ega biometrik parametрни ko'rsating.

a. Ko'z qorachig'i

b. Yuz tasviri

c. Barmoq izi

d. Qo'l shakli

**71) Agar har ikkala tomonning haqiqiyligini tekshirish jarayoni bu?**

**a. Ikki tomonlama autentifikatsiya**

b. Ikki faktorli autentifikatsiya

c. Ko'p faktorli autentifikatsiya

d. Biometrik autentifikatsiya

**72) Ko'p faktorli autentifikatsiya bu?**

**a. S va D javoblar to'g'ri**

b. Har ikkala tomonni haqiqiyligini tekshirish darayoni

c. Birdan ortiq faktorlardan foydalanish asosida haqiqiylikni tekshirish

d. Barmoq izi va parol asosida haqiqiylikni tekshirish

**73) Biror narsani bilishga asoslangan**

**autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating?**

**a. Parollar lug'atidan foydalanish asosida hujum, elka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum**

b. Fizik o'g'irlash hujumi, elka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum

- c. Parollar lug'atidan foydalanish asosida hujum, elka orqali qarash hujumi, qalbakilashtirish
- b. hujumi
- a. Parollar lug'atidan foydalanish asosida hujum, bazadagi parametрни almashtirish hujumi, zararli dasturlardan foydanish asosida hujum

**74) Biror narsaga **egalik qilishga** asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating?**

- a. **Fizik o'g'irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar**
- b. Parollar lug'atidan foydalanish asosida hujum, elka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum
- c. Fizik o'g'irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar
- d. Parollar lug'atidan foydalanish asosida hujum, bazadagi parametрни almashtirish hujumi, zararli dasturlardan foydanish asosida hujum



**75) Biometrik parametrga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating?**

**a. Qalbakilashtirish, ba'lumotlar bazasidagi parametrlarni almashtirish**

- b. Fizik o'g'irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar
- c. Fizik o'g'irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar
- d. Qalbakilashtirish, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar

**76) Parollar bazada qanday ko'rinishda saqlanadi?**

**a. Xeshlangan ko'rinishda**

- b. Shifrlangan ko'rinishda
- c. Ochiq holatda
- d. Bazada saqlanmaydi

**77) Agar parolning uzunligi 8 ta belgi va har bir o'rinda 256 ta turlicha belgidan foydalanish**

mumkin bo'lsa, bo'lishi mumkin jami parollar sonini toping.

a. 2568

b. 8256

c. 256!

d. 2256

2568

78) Parolni "salt" (tuz) kattaligidan foydalanib xeshlashdan ( $h(\text{password}, \text{salt})$ ) asosiy maqsad nima?

a. Buzg'unchiga ortiqcha hisoblashni talab etuvchi murakkablikni yaratish

b. Buzg'unchi topa olmasligi uchun yangi nomalum kiritish

c. Xesh qiymatni tasodifiylik darajasini oshirish

d. Xesh qiymatni qaytmaslik talabini oshirish

79) Qanday paroldan foydalanish tavsiya etiladi?

a. Iboralar asosida hosil qilingan parollardan

b. Turli belgidan iborat va murakkab parollardan

c. Faqat belgi va raqamdan iborat parollardan

d. Faqat raqamdan iborat parollardan

80) **Fizik** himoyani buzilishiga olib keluvchi tahdidlar yuzaga kelish shakliga ko'ra qanday guruhlarga bo'linadi?

a. Tabiiy va sun'iy

b. Ichki va tashqi

c. Aktiv va passiv

d. Bir tomonlama va ko'p tomonlama

81) Quyidagilarnig qaysi biri **tabiiy tahdidlar** hisoblanadi?

a. Yong'in, suv toshishi, harorat ortishi

b. Yong'in, o'g'irlik, qisqa tutashuvlar

c. Suv toshishi, namlikni ortib ketishi, bosqinchilik

d. Bosqinchilik, terrorizm, o'g'irlik

82) Quyidagilarnig qaysi biri **sun'iy tahdidlar** hisoblanadi?

a. Bosqinchilik, terrorizm, o'g'irlik

b. Yong'in, suv toshishi, harorat ortishi

c. Yong'in, o'g'irlik, qisqa tutashuvlar

d. Suv toshishi, namlikni ortib ketishi, bosqinchilik

**83) Yong'inga qarshi kurashishning **passiv** usuliga kiruvchi choralarni ko'rsating**

**a. Yong'inga chidamli materiallardan foydalanish, zaxira xona va etajlarni qoldirish, tushuntiruv ishlarini olib borish**

b. Yong'inni aniqlash, agnishitel va qum yordamida o'chirish

c. Yong'inga chidamli materiallardan foydalanish, agnishitel va qum yordamida o'chirish

d. Zaxira xona va etajlarni qoldirish, tushuntiruv ishlarini olib borish, yong'in bo'lganligi haqida signal berish

**84) Axborotni **fizik xavfsizligini** ta'minlashda inson faktorini **mujassamlashtirgan** nazoratlash usuli bu?**

**a. Ma'muriy nazoratlash**

b. Fizik nazoratlash

c. Texnik nazoratlash

d. Apparat nazoratlash

**85) Qaysi **fizik to'siq** insonlarni tashkilotda faqat bittadan kirishini ta'minlaydi?**

**a. Turniket**

b. To'mba

- c. Metal zaborlar
- d. Elektr zaborlar

**86) Faqat ob'ektning egasi tomonidan foydalanish imtiyozini nazoratlaydigan mantiqiy foydalanish usuli bu?**

**a. Diskretsiyon foydalanishni boshqarish**

- b. Mandatli foydalanishni boshqarish
- c. Rolga asoslangan foydalanishni boshqarish
- d. Attributga asoslangan foydalanishni boshqarish

**87) Ob'ektlar va sub'ektlarni klassifikatsiyalashga asoslangan foydalanishni boshqarish usuli bu?**

**a. Mandatli foydalanishni boshqarish**

- b. Diskretsiyon foydalanishni boshqarish
- c. Rolga asoslangan foydalanishni boshqarish
- d. Attributga asoslangan foydalanishni boshqarish

**88) 1. Agar sub'ektning xavfsizlik darajasida ob'ektning xavfsizlik darajasi mavjud bo'lsa, u holda o'qish uchun ruxsat beriladi; 2. Agar sub'ektning xavfsizlik darajasi ob'ektning xavfsizlik**

darajasida bo'lsa, u holda **yo'zishga** ruxsat beriladi.  
Ushbu qoidalar axborotni qaysi xususiyatini  
ta'minlashga qaratilgan?

**a. Konfidensiallikni**

b. Foydalanuvchanlikni

c. Butunlikni

d. Ishonchlilikni

**89) 1. Agar sub'ektning xavfsizlik darajasida ob'ektning xavfsizlik darajasi mavjud bo'lsa, u holda **yo'zish** uchun ruxsat beriladi. 2. Agar sub'ektning xavfsizlik darajasi ob'ektning xavfsizlik darajasida bo'lsa, u holda **o'qishga** ruxsat beriladi.**  
Ushbu qoidalar axborotni qaysi xususiyatini  
ta'minlashga qaratilgan?

**a. Butunlikni**

b. Konfidensiallikni

c. Foydalanuvchanlikni

d. Maxfiylikni

90) Foydalanishni **boshqarishni** tashkilotlardagi kadrlar toifasiga maksimal darajada yaqinlashtirishga harakat qilgan usul bu?

a. Rolga asoslangan foydalanishni boshqarish

b. Mandatli foydalanishni boshqarish

c. Diskretsiya foydalanishni boshqarish

d. Attributga asoslangan foydalanishni boshqarish

91) Muayyan **faoliyat turi bilan bog'liq** harakatlar va majburiyatlar to'plami bu?

a. Rol

b. Imtiyoz

c. Daraja

d. Imkoniyat

92) **Qoida** (rules), **siyosat** (policy), qoida va siyosatni mujassamlashtirgan algoritmlar (rule-combining algorithms), majburiyatlar (obligations) va maslahatlar (advices) kabi tushunchalar qaysi foydalanishni boshqarish usuliga aloqador.

a. Attributga asoslangan foydalanishni boshqarish

- b. Rolga asoslangan foydalanishni boshqarish
- c. Mandatli foydalanishni boshqarish
- d. Diskretsion foydalanishni boshqarish

**93) Ushbu keltirilgan shart qaysi foydalanishni boshqarish usuliga tegishli:**

**sub'ekt.Lavozimi=Vrach & muhit.vaqtl >= 8:00 & muhit.vaqtl <=18:00**

**a. Attributga asoslangan foydalanishni boshqarish**

- b. Rolga asoslangan foydalanishni boshqarish
- c. Mandatli foydalanishni boshqarish
- d. Diskretsion foydalanishni boshqarish

**94) Sug'urta ma'lumotiga tegishli bo'lgan .... quyidagicha:**

**(Bob,),(Alisa,rw),(Sem,rw),(buxgalteriyaga oid dastur,rw). Nuqtalar o'rniga mos atamani qo'ying.**

**a. Foydalanishni boshqarish ro'yxati yoki ACL**

- b. Imtiyozlar ro'yxati yoki C-list
- c. Foydalanishni boshqari matritsasi
- d. Biba modeli



**95) Alisaga tegishli ... quyidagiga teng:**

**(OT,rx),(,buxgalteriyaga oid**

**dastur,rx),(buxgalteriyaga oid ma'lumot,r).**

**Nuqtalar o'rniga mos atamani qo'ying.**

**a. Imtiyozlar ro'yxati yoki C-list**

b. Foydalanishni boshqarish ro'yxati yoki ACL

c. Foydalanishni boshqari matritsasi

d. Biba modeli

**96) Foydalanishni boshqarish matritsani ustunlar**

**bo'yicha bo'lish va har bir ustunni mos ob'ekt bilan**

**saqlash orqali .... hosil qilinadi. Nuqtalar o'rniga**

**mos atamani qo'ying.**

**a. Foydalanishni boshqarish ro'yxati yoki ACL**

b. Imtiyozlar ro'yxati yoki C-list

c. Foydalanishni boshqari matritsasi

d. Biba modeli

**97) Foydalanishni boshqarish matritsasini satrlar**

**bo'yicha saqlash va har bir satr mos sub'ekt bilan**

saqlash orqali .... hosil qilinadi. Nuqtalar o'rniga mos atamani qo'ying.

a. Imtiyozlar ro'yxati yoki C-list

b. Foydalanishni boshqarish ro'yxati yoki ACL

c. Foydalanishni boshqari matritsasi

d. Biba modeli

98) Bell-Lapadula modeli axborotni qaysi xususiyatini ta'minlashni maqsad qiladi?

a. Konfidensiallik

b. Butunlik

c. Foydalanuvchanlik

d. Ishonchlilik

99) Biba modeli axborotni qaysi xususiyatini ta'minlashni maqsad qiladi?

a. Butunlik

b. Konfidensiallik

c. Foydalanuvchanlik

d. Maxfiylik

**100) Biba modeliga ko'ra agar birinchi ob'ektning ishonchlilik darajasi  $I(O1)$  ga teng bo'lsa va ikkinchi ob'ektning ishonchlilik darajasi  $I(O2)$  ga teng bo'lsa, u holda ushbu ikkita ob'ektdan iborat bo'lgan uchinchi ob'ektning ishonchlilik darajasi nimaga teng bo'ladi? Bu yerda,  $I(O1) > I(O2)$ .**

**a.  $I(O2)$**

b.  $I(O1)$

c.  $I(O2)$  va  $I(O2)$  ga bog'liq emas

d. Berilgan shartlash yetarli emas

**101) Bell- Lapadula modeliga modeliga ko'ra agar birinchi ob'ektning xavfsizlik darajasi  $L(O1)$  ga teng bo'lsa va ikkinchi ob'ektning xavfsizlik darajasi  $L(O2)$  ga teng bo'lsa, u holda ushbu ikkita ob'ektdan iborat bo'lgan uchinchi ob'ektning xavfsizlik darajasi nimaga teng bo'ladi? Bu yerda,  $L(O1) > L(O2)$ .**

**a.  $L(O1)$**

- b.  $L(O_2)$
- c.  $L(O_1)$  va  $L(O_2)$  ga bog'liq emas
- d. Berilgan shartlar yetarli emas

**102) Agar biz  $O_1$  ob'ektning butunligiga ishonsak, biroq  $O_2$  ob'ektning butunligiga ishonmasak, u holda ob'ekt  $O$  ikkita  $O_1$  va  $O_2$  ob'ektlardan yaratilgan bo'lsa, u holda ob'ekt  $O$  ning butunligiga ishonmaymiz. Bu qaysi modelni anglatadi?**

**a. Biba modelini**

- b. Bell-Lapadula modelini
- c. Biror bir modelga tegishli emas
- d. Biba va Bell-Lapadula modellari kombinatsiyasini.

**103) “Protsessorda shifrlash kalitini generatsiya qilish uchun maxsus kalit generatori mavjud bo' lib, foydalanuvchi kiritgan parol asosida qulfdan yechiladi”. Gap qaysi turdagi shifrlash vositasi haqidi ketmoqda.**

**a. Apparat**

- b. Dasturiy

- c. Simmetrik
- d. Ochiq kalitli

**104) “Shifrlashda boshqa dasturlar kabi kompyuter resursidan foydalanadi”. Gap qaysi turdagi shifrlash vositasi haqidi ketmoqda.**

- a. Dasturiy**
- b. Apparat
- c. Simmetrik
- d. Ochiq kalitli

**105) Dasturiy ko‘rinishdagi shifrlash vositasi uchun mos bo‘lgan xususiyatni belgilang.**

- a. Yangilash imkoniyati mavjud.**
- b. Shifrlash uchun saqlagishdagi (qurilmada) joylashgan maxsus protsessordan foydalanadi
- c. Autentifikatsiya apparat qurilmaga nisbatan amalga oshiriladi
- d. Qo‘shimcha drayver yoki dasturlarni o‘rnatishning hojati yo‘q

**106) Apparat ko‘rinishdagi shifrlash vositasi uchun mos bo‘lmagan xususiyatni belgilang.**

- a. Yangilash imkoniyati mavjud.**

- b. Shifrlash uchun saqlagishdagi (qurilmada) joylashgan maxsus protsessordan foydalanadi
- c. Autentifikatsiya apparat qurilmaga nisbatan amalga oshiriladi
- d. Qo'shimcha drayver yoki dasturlarni o'rnatishning hojati yo'q

**107) Apparat ko'rinishdagi shifrlash vositasi uchun mos bo'lgan xususiyatni belgilang.**

**a. Qo'shimcha drayver yoki dasturlarni o'rnatishning hojati yo'q**

- b. Yangilash imkoniyati mavjud.
- c. Parolni to'liq tanlash hujumi yoki parolni topishga qaratilgan boshqa hujumlarga bardoshsiz
- d. Foydalanuvchi tomonidan kiritilgan parol ma'lumotni shifrlash kaliti sifatida foydalaniladi

**108) Diskni shifrlash usuliga xos bo'lgan xususiyatlarni belgilang.**

**a. Deyarli barcha narsa, almashtirish maydoni (swap space), vaqtinchalik fayllar, shifrlanadi.**

- b. Kalitlarni boshqarish, ya'ni, har bir fayl uchun turli kalitlardan foydalanish mumkin.

- c. Faqat kriptografik kalitlar xotirada saqlanib, shifrlangan fayllar ochiq holatda saqlanadi.
- d. asosiy fayl tizimining ustida joylashgan kriptografik fayl tizimidan foydalanish (masalan, ZFS, EncFS).

**109) Faylni shifrlash usuliga xos bo'lgan xususiyatlarni belgilang.**

- a. Kalitlarni boshqarish, ya'ni, har bir fayl uchun turli kalitlardan foydalanish mumkin.
- b. Foydalanuvchi shaxsiy xabarlarni alohida shifrlashni unutgan vaqtlarda juda qo'l keladi.
- c. Zudlik bilan ma'lumotlarni yo'q qilish uchun o'rinli.
- d. Deyarli barcha narsa, almashtirish maydoni (swap space), vaqtinchalik fayllar, shifrlanadi.

**110 Ma'lumotni xavfsiz yo'q qilish nima uchun zarur?**

- a. Ma'lumotni to'liq konfidensialligini ta'minlash uchun
- b. Ma'lumotni butunligini ta'minlash uchun
- c. Ma'lumotni foydalanuvchanligini ta'minlash uchun
- d. Xotirani bo'shatish uchun.

**111) Qog'oz ko'rinishdagi ma'lumotni yo'q qilish usullari orasidan quriq iqlimli sharoit uchun mos bo'lmaganini aniqlang.**

**a. Ko'mish**

b. Yoqish

c. Kimyoviy usul

d. maydalash (shreder)

**112) Ekologiyaga salbiy tasir qiluvchi, ortiqcha xarajatlarni talab etuvchi qog'oz ko'rinishdagi ma'lumotlarni yo'q qilish usulini aniqlang.**

**a. Yoqish**

b. Ko'mish

c. Kimyoviy usul

d. maydalash (shreder)

**113) Recuva, Wise Data Recovery, PC Inspector File Recovery, EaseUS Data Recovery Wizard Free, TestDisk and PhotoRec. Ushbu nomlarga xos bo'lgan umumiy xususiyatni toping.**

**a. Ularning barchasi ma'lumotni tiklovchi dasturiy vositalar.**



- b. Ularning barchasi bepul foydalaniluvchi dasturiy vositalar.
- c. Ularning barchasi ma'lumotni xavfsiz o'chiruvchi dasturiy vositalar.
- d. Ularning barcha ma'lumotlarni zaxira saqllovchi dasturiy vositalar.

**114) Kriptografik kalit uzunligining o'lchov birligi?**

**a. Bit**

- b. Belgilar soni, ya'ni, ta
- c. Kbayt
- d. Metr

**115) Parol uzunligining o'lchov birligi?**

**a. Belgilar soni, ya'ni, ta**

- b. Bit
- c. Kbayt
- d. Metr

**116) Yaratish uchun biror matematik muammoni talab etadigan shifrlash algoritmi?**

**a. Ochiq kalitli shifrlar**

- b. Simmetrik shifrlar
- c. Blokli shifrlar

d. Oqimli shifrlar

**117) Xesh funksiyalarda kolliziya hodisasi bu - ?**

**a. Ikki turli matnlarning xesh qiymatlarini bir xil bo'lishi**

b. Cheksiz uzunlikdagi axborotni xeshlay olishi

c. Tezkorlikda xeshlash imkoniyati

d. Turli matnlar uchun turli xesh qiymatlarni hosil bo'lishi

**118) Xeshlangan ma'lumot nima deb ataladi?**

**a. Xesh qiymat**

b. Kalit

c. Shifrmavn

d. Parol

**119) Parol kalitdan nimasi bilan farq qiladi?**

**a. Tasodifiylik darajasi bilan**

b. Uzunligi bilan

c. Belgilari bilan

d. Samaradorligi bilan

**120) 26 ta belgidan iborat Sezar shifrlash usilida**

**kalitni bilmasdan turib nechta urinishda ochiq  
matnni aniqlash mumkin?**

a. 25

b. 26!

c. 13

d. 252

**121) Elektron raqamli imzoni muolajalarini ko'rsating?**

a. Imzoni shakllantirish va imkoni tekshirish

b. Shifrlash va deshifrlash

c. Imzoni xeshlash va xesh matnni deshifrlash

d. Imzoni shakllantirish va xeshlash

**122) "Elka orqali qarash" hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.**

a. Biror narsani bilishga asoslangan autentifikatsiya.

b. Biror narsaga egalik qilishga asoslangan autentifikatsiya.

c. Biometrik autentifikatsiya.

d. Tokenga asoslangan autentifikatsiya

**123) Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan.**

a. Biror narsani bilishga asoslangan autentifikatsiya.

- b. Biror narsaga egalik qilishga asoslangan autentifikatsiya.
- c. Biometrik autentifikatsiya.
- d. Tokenga asoslangan autentifikatsiya

**124) Yo'qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon.**

**a. Biror narsani bilishga asoslangan autentifikatsiya.**

- b. Biror narsaga egalik qilishga asoslangan autentifikatsiya.
- c. Biometrik autentifikatsiya.
- d. Tokenga asoslangan autentifikatsiya

**125) Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.**

**a. Biometrik autentifikatsiya.**

- b. Biror narsani bilishga asoslangan autentifikatsiya.
- c. Biror narsaga egalik qilishga asoslangan autentifikatsiya.
- d. Tokenga asoslangan autentifikatsiya

**126) Elektron axborot saqlovchilardan qayta foydalanishli ma'lumotlarni yo'q qilish usullarini aniqlang.**

**a. Qayta yozish va formatlash**

- b. Fizik yo'q qilish
- c. Maydalash (shredirlash)
- d. Yanchish

**127) Elektron axborot saqlovchilardan ma'lumotni yo'q qilishning qaysi usuli to'liq kafolatlangan.**

**a. Fizik yo'q qilish**

- b. Qayta yozish
- c. Formatlash
- d. O'chirish

**128) Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?**

**a. Axborot xavfsizligi buzulgan taqdirda ko'rilishi mumkin bo'lgan zarar miqdori bilan**

- b. Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhurligi bilan
- c. Axborotni noqonuniy foydalanishlardan, o'zgartirishlardan va yo'q qilishlardan himoyalanganligi bilan
- d. Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bilan

**129) Axborotdan qanday foydalanish ruxsat etilgan deb yuritiladi?**

- a. Foydalanishga o'rnatilgan chegaralash qoidalarini buzmaydigan**
- b. Foydalanishga o'rnatilgan chegaralash qoidalarini buzadigan
- c. Axborot butunligini buzmaydigan
- d. Axborot konfidensialligini buzmaydigan

**130) Axborotni butunligini ta'minlash usullarini ko'rsating.**

- a. Xesh funksiyalar, MAC**
- b. Shifrlash usullari.
- c. Assimetrik shifrlash usullari, CRC tizimlari.
- d. Shifrlash usullari, CRC tizimlari.

**131) Biba modeliga ko'ra agar birinchi ob'ektning ishonchlilik darajasi  $I(O1)$  ga teng bo'lsa va ikkinchi ob'ektning ishonchlilik darajasi  $I(O2)$  ga teng bo'lsa, u holda ushbu ikkita ob'ektdan iborat bo'lgan uchinchi ob'ektning ishonchlilik darajasi nimaga teng bo'ladi?**

Bu yerda,  $I(O1) < I(O2)$ .

a.  $I(O1)$

b.  $I(O2)$

c.  $I(O2)$  va  $I(O2)$  ga bog'liq emas

d. Berilgan shartlash yetarli emas

**132) Biba modeliga ko'ra agar birinchi ob'ektning ishonchlilik darajasi  $I(O1)$  ga, ikkinchi ob'ektning ishonchlilik darajasi  $I(O2)$  ga va uchinchi ob'ektning ishonchlilik darajasi  $I(O3)$  teng bo'lsa, u holda ushbu uchta ob'ektdan iborat bo'lgan to'rtinchi ob'ektning ishonchlilik darajasi nimaga teng bo'ladi?**

Bu yerda,  $I(O1) > I(O2) > I(O3)$ .

a.  $I(O3)$

b.  $I(O2)$

c.  $I(O1)$

d. Berilgan shartlash yetarli emas

**133) Bell- Lapadula modeliga modeliga ko'ra agar birinchi ob'ektning xavfsizlik darajasi  $L(O1)$  ga teng**

bo'lsa va ikkinchi ob'ektning xavfsizlik darajasi  $L(O_2)$  ga teng bo'lsa, u holda ushbu ikkita ob'ektdan iborat bo'lgan uchinchi ob'ektning xavfsizlik darajasi nimaga teng bo'ladi?

Bu yerda,  $L(O_1) < L(O_2)$ .

a.  $L(O_2)$

b.  $L(O_1)$

c.  $L(O_1)$  va  $L(O_2)$  ga bog'liq emas

d. Berilgan shartlar yetarli emas

134) Bell- Lapadula modeliga modeliga ko'ra agar birinchi ob'ektning xavfsizlik darajasi  $L(O_1)$  ga, ikkinchi ob'ektning xavfsizlik darajasi  $L(O_2)$  ga va uchinchi ob'ektning xavfsizlik darajasi  $L(O_3)$  teng bo'lsa, u holda ushbu uchta ob'ektdan iborat bo'lgan to'rtinchi ob'ektning xavfsizlik darajasi nimaga teng bo'ladi?

Bu yerda,  $L(O_1) < L(O_2) < L(O_3)$ .

a.  $L(O_3)$



- b. L(O1)
- c. L(O2)
- d. Berilgan shartlar yetarli emas

**135) Elektron axborot saqllovchilardan qayta foydalanishli ma'lumotlarni yo'q qilish usullari orasidan eng ishonchlisini aniqlang.**

**a. Takroriy qayta yozish**

- b. Formatlash
- c. Shift+Delete buyrug'i yordamida o'chirish
- d. Delete buyrug'i yordamida o'chirish

**136) Quyida keltirilganlarning orasidan kompyuter topologiyalari hisoblanmaganlarini aniqlang.**

**a. LAN, GAN, OSI**

- b. Yulduz, WAN, TCP/IP
- c. Daraxt, IP, OSI
- d. Shina, UDP, FTP

**137) OSI tarmoq modeli nechta sathdan iborat?**

**a. 7**

- b. 4
- c. 6

d. 5

**138) TCP/IP tarmoq modeli nechta sathdan iborat?**

**a. 4**

b. 7

c. 6

d. 5

**139) Quyidagilar orasidan qaysilari tarmoq turlari emas?**

**a. Yulduz, WAN, TCP/IP**

b. LAN, GAN

c. WAN, MAN

d. PAN, CAN

**140) Hajmi bo'yicha eng kichik hisoblangan tarmoq turini ko'rsating?**

**a. PAN**

b. LAN

c. CAN

d. MAN

**141) Qaysi topologiyada tarmoqdagi bir ishchi uzelnig ishdan chiqishi butun tarmoqni ishdan chiqishiga sababchi bo'лади.**

**a. Halqa topologiyada**

b. Yulduz topologiyada

c. Shina topologiyada

d. Mesh topologiyada

**142) IPv4 protokolida IP manzil uchun necha bit ajratiladi.**

**a. 32**

b. 64

c. 128

d. 4

**143) IPv6 protokolida IP manzil uchun necha bit ajratiladi.**

**a. 128**

b. 32

c. 64

d. 4

**144) Domen nomlarini IP manzilga yoki aksincha almashtirishni amalga oshiruvchi xizmat bu?**

**a. DNS**

b. TCP/IP

c. OSI

d. UDP

**145) Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi va ularni uzib qo'yuvchi oshkor bo'lmagan hodisalarning potensial paydo bo'lishi bu?**

**a. Tahdid**

b. Zaiflik

c. Hujum

d. Aktiv

**146) "Portlaganida" tizim xavfsizligini buzuvchi kutilmagan va oshkor bo'lmagan hodisalarga olib keluvchi kamchilik, loyihalashdagi yoki amalga oshirishdagi xatolik bu?**

**a. Zaiflik**

- b. Tahdid
- c. Hujum
- d. Kamchilik

**147) Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat bu?**

**a. Hujum**

- b. Zaiflik
- c. Tahdid
- d. Zararli harakat

**148) Tarmoq xavfsizligi muammolariga olib kelmaydigan sababni aniqlang.**

**a. Routerlardan foydalanmaslik**

- b. Qurilma yoki dasturiy vositani noto'g'ri sozlanishi
- c. Tarmoqni xavfsiz bo'lmagan tarzda va zaif loyihalash
- d. Tug'ma texnologiya zaifligi

**149) Tashkilot ichidan turib, xafa bo'lgan xodimlar, g'araz niyatli xodimlar tomonidan amalga oshirilishi mumkin bo'lgan tahdidlar bu?**

**a. Ichki tahdidlar**

- b. Tashqi tahdidlar
- c. Maxsus tahdidlar
- d. Qastdan qilingan tahdidlar

## **150) Tarmoq xavfsizligini buzilishi biznes faoliyatga qanday ta'sir qiladi?**

- a. Biznes faoliyatning buzilishi, huquqiy javobgarlik**
- b. Axborotni o'g'irlanishi, tarmoq qurilmalarini fizik buzilishiga olib keladi
- c. Maxfiylikni yo'qolishi, tarmoq qurilmalarini fizik buzilishiga olib keladi
- d. Huquqiy javobgarlik, tarmoq qurilmalarini fizik buzilishiga olib keladi

## **151) Razvedka hujumlari bu?**

- a. Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi.**
- b. Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.
- c. Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.

d. Tizimni fizik buzishni maqsad qiladi.

$\langle \text{I}(\text{o}2) \text{I}(\text{o}3) \rangle \langle \text{I}(\text{o}2) \rangle \langle \text{I}(\text{o}2) \rangle$

## 152) Kirish hujumlari bu?

**a. Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.**

b. Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi.

c. Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.

d. Tarmoq haqida axborotni to'plash hujumchilarga mavjud bo'lgan potensial zaiflikni aniqlashga harakat qiladi.

## 153) Xizmatdan vos kechishga qaratilgan hujumlar bu?

**a. Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.**

b. Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.

c. Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi.

d. Tarmoq haqida axborotni to'plash hujumchilarga mavjud bo'lgan potensial zaiflikni aniqlashga harakat qiladi.

**154) Paketlarni snifferlash, portlarni skanerlash va Ping buyrug'ini yuborish hujumlari qaysi hujumlar toifasiga kiradi?**

**a. Razvedka hujumlari**

b. Kirish hujumlari

c. DOS hujumlari

d. Zararli dasturlar yordamida amalga oshiriladigan hujumlar.

**155) “Bir qarashda yaxshi va foydali kabi ko'rinuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi”. Bu xususiyat qaysi zararli dastur turiga xos.**

**a. Trojan otlari.**

b. Adware

c. Spyware

d. Backdoors

**156) “Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish**



**rejimini kuzutib boradi”. Bu xususiyat qaysi zararli dastur turiga xos.**

**a. Adware**

b. Trojan otlari.

c. Spyware

d. Backdoors

**157) “Hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi”.**

**Bu xususiyat qaysi zararli dastur turiga xos.**

**a. Backdoors**

b. Adware

c. Trojan otlari.

d. Spyware

**158) “Foydalanuvchi ma’lumotlarini qo’lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod”. Bu xususiyat qaysi zararli dastur turiga xos.**

**a. Spyware**

- b. Backdoors
- c. Adware
- d. Trojan otlari.

**159) “Biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi”. Bu xususiyat qaysi zararli dastur turiga xos.**

**a. Backdoors**

- b. Adware
- c. Trojan otlari.

**160) “Obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi”. Bu xususiyat qaysi zararli dastur turiga xos.**

**a. Botnet**

- b. Backdoors
- c. Adware
- d. Trojan otlari.

**161 “Qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga**

**oshirilishini talab qiladi". Bu xususiyat qaysi zararli dastur turiga xos.**

**a. Ransomware**

- b. Backdoors
- c. Adware
- d. Trojan otlari.

**162) Umumiy tapmoqni ikki qismga: ichki va tashqi tapmokga ajapatuvchi himoya vositasi bu?**

**a. Tapmoklararo ekran**

- b. Antivirus
- c. Virtual himoyalangan tarmoq
- d. Router

**163) Paket filterlari turidagi tarmoqlararo ekran vositasi OSI modelining qaysi sathida ishlaydi?**

**a. Tarmoq sathida**

- b. Transport sathida
- c. Ilova sathida
- d. Kanal sathida

**164) Tashqi tapmokdagi foydalonuvchilapdan ichki tapmok pesupslapini ximoyalash qaysi tarmoq himoya vositasining vazifasi hisoblanadi.**

**a. Tarmoqlararo ekran**

- b. Antivirus
- c. Virtual himoyalangan tarmoq
- d. Router

**165) Ichki tarmok foydalanuvchilarini tashqi tarmoqqa bo'lgan murojaatlarini chegaralash qaysi tarmoq himoya vositasining vazifasi hisoblanadi.**

**a. Tarmoqlararo ekran**

- b. Antivirus
- c. Virtual himoyalangan tarmoq
- d. Router

166) Qaysi tarmoq himoya vositasi tapmok manzili, identifikatorlar, interfeys manzili, popt nomeri va boshqa parametrlar yordamida filterlashni amalga oshiradi.

**a. Tarmoqlararo ekran**

- b. Antivirus
- c. Virtual himoyalangan tarmoq

d. Router

**167) Ikki uzel opasida axbopotni konfidensiyalligini va butunligini ta'minlash uchun himoyalangan tunelni quruvchi himoya vositasi bu?**

**a. Virtual Private Network**

b. Tapmoklapapo ekpan

c. Antivirus

d. Router

**168) Qaysi himoya vositasi tarmoqda uzatilayotgan axborotni butunligi, maxfiyligi va tomonlar autentifikatsiyasini ta'minlaydi?**

**a. Virtual Private Network**

b. Tapmoklapapo ekpan

c. Antivirus

d. Router

**169) Qaysi himoya vositasida mavjud paket shifplangan xolda yangi hosil qilingan mantiqiy paket ichiga kiritiladi?**

**a. Virtual Private Network**

- b. Tapmoklapapo ekpan
- c. Antivirus
- d. Router

**170) Virtual xususiy tarmoq OSI modelining kanal sathida qaysi protokollar yordamida amalga oshiriladi?**

**a. L2F, L2TP**

- b. PPTP, TLS
- c. TLS, TCP
- d. L2TP, IP

171) Virtual xususiy tarmoq OSI modelining tarmoq sathida qaysi protokol yordamida amalga oshiriladi?

**a. IPSec**

- b. L2TP
- c. TCP
- d. PPTP

**172) Virtual xususiy tarmoq OSI modelining seans sathida qaysi protokol yordamida amalga oshiriladi?**

- a. TLS

- b. L2TP
- c. TCP
- d. PPTP

**173) Ochiq tapmok yordamida ximoyalangan tapmokni qupish imkoniyatiga ega himoya vositasi bu?**

**a. Virtual Private Network**

- b. Tapmoklapapo ekpan
- c. Antivirus
- d. Router

**174) “Mavjud bo‘lgan IP - paket to‘liq shifplanib, unga yangi IP soplavha bepiladi”. Ushbu amal qaysi himoya vositas**

**i tomonidan amalga oshiriladi.**

**a. Virtual Private Network**

- b. Tapmoklapapo ekpan
- c. Antivirus
- d. Router

**175) Foydalanuvchi tomonidan kiritilgan taqiqlangan so'rovni qaysi himoya vositasi yordamida nazoratlash mumkin.**

**a. Tarmoqlararo ekran**

b. Virtual Private Network

c. Antivirus

d. Router

**176) Qaysi himoya vositasi tomonlarni autentifikatsiyalash vazifasini amalga oshiradi.**

**a. Virtual Private Network**

b. Tapmoklapapo ekpan

c. Antivirus

d. Router

**177) Qaysi himoya vositasi etkazilgan axbopotni butunligini va to'g'riligini tekshirish vazifasini amalga oshiradi.**

**a. Virtual Private Network**

b. Tapmoklapapo ekpan

c. Antivirus



d. Router

**178) Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga imkon beruvchi himoya vositasi bu?**

a. Tarmoqlararo ekran

b. Virtual Private Network

c. Antivirus

d. Router

**179) Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?**

a. Texnik vositalarning buzilishi va ishlamasligi

b. Axborotdan ruhsatsiz foydalanish

c. Zararkunanda dasturlar

d. An'anaviy josuslik va diversiya

**180) Axborotni deshifrlash deganda qanday jarayon tushuniladi?**

a. Yopiq axborotni kalit yordamida ochiq axborotga

o'zgartirish

b. Saqlanayotgan sirli ma'lumotlarni tarqatish

c. Tarmoqdagi ma'lumotlardan ruxsatsiz foydalanish

d. Tizim resurslariga noqonuniy ulanish va foydalanish

## **181) Axborotni qanday ta'sirlardan himoyalash kerak?**

**a. Axborotdan ruxsatsiz foydalanishdan, uni buzilishdan yoki yo'q qilinishidan**

b. Axborotdan qonuniy foydalanishdan, uni qayta ishlash yoki sotishdan

c. Axborotdan qonuniy foydalanishdan, uni qayta ishlash yoki foydalanishdan

d. Axborotdan tegishli foydalanishdan, uni tarmoqda uzatishdan

## **182) Axborotni maxfiyligini ta'minlashda quyidagi algoritmlardan qaysilari foydalaniladi?**

**a. RSA, DES, AES**

b. AES, CRC, SHA1

c. MD5, DES, ERI

d. ERI, MAC, SHA2

**183) Axborotni uzatish va saqlash jarayonida o'z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?**

**a. Ma'lumotlar butunligi**

- b. Axborotning konfidensialligi
- c. Foydalanuvchanligi
- d. Ixchamligi

**184) Axborotni foydalanuvchanligini buzushga qaratilgan tahdidni aniqlang.**

**a. DDOS tahdidlar**

- b. Nusxalash tahdidlari
- c. Modifikatsiyalash tahdidlari
- d. O'rta turgan odam tahdidi

**185) Axborotni shifrlash deganda qanday jarayon tushuniladi?**

**a. Ochiq axborotni kalit yordamida yopiq axborotga o'zgartirish**

- b. Kodlangan malumotlarni yig'ish
- c. Axborotlar o'zgartirish jarayoni

d. Jarayonlar ketma-ketligi

## **186) Virtual himoyalangan tunnelning asosiy afzalligi-bu?**

**a. Tashqi faol va passiv kuzatuvchilarning foydalanishi juda qiyinligi**

b. Tashqi faol va passiv kuzatuvchilarning foydalanishi juda oddiyligi

c. Tashqi faol va passiv kuzatuvchilarning foydalanishi juda qulayligi

d. Tashqi faol va passiv kuzatuvchilarning foydalanish imkoniyati ko'pligi

## **187) Global simsiz tarmoqning ta'sir doirasi qanday?**

**a. Butun dunyo bo'yicha**

b. Binolar va korpuslar

c. O'rtacha kattalikdagi shahar

d. Foydalanuvchi yaqinidagi tarmoq

## **188) Dinamik parol-bu:**

**a. Bir marta ishlatiladigan parol**

b. Ko'p marta ishlatiladigan parol

c. Foydalanuvchi ismi

d. Murakkab parol

**189) Eng ko'p foydalaniladigan autentifikatsiyalash asosi-bu:**

**a. Parolga asoslangan**

b. Tokenga asoslangan

c. Biometrik parametrlarga asoslangan

d. Smart kartaga asoslangan

**190) Zararli dasturlarni ko'rsating?**

**a. Kompyuter viruslari va mantiqiy bombalar**

b. Letsenziyasiz dasturlar va qurilmalar

c. Tarmoq kartasi va dasturlar

d. Internet tarmog'i dasturlari

**191) RSA shifrlash algoritmida tanlangan p va q sonlarga qanday talab qo'yiladi?**

**a. Tub bo'lishi**

b. O'zaro tub bo'lishi

c. Butun son bo'lishi

d. Toq son bo'lishi

**192) 12 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?**

**a. 5,7,11**

b. 13,4,7

c. 11,2,5

d. 13,11,10

**193) Bluetooth standarti qaysi simsiz tarmoq turiga qiradi?**

**a. Shaxsiy simsiz tarmoq**

b. Lokal simsiz tarmoq

c. Mintaqaviy simsiz tarmoq

d. Global simsiz tarmoq

**194) Parolga "tuz"ni qo'shib xeshlashdan maqsad?**

**a. Tahdidchi ishini oshirish**

b. Murakkab parol hosil qilish

c. Murakkab xesh qiymat hosil qilish

d. Ya'na bir maxfiy parametr kiritish

**195) Parol kalitdan nimasi bilan farq qiladi?**

**a. Tasodifiylik darajasi bilan**

- b. Uzunligi bilan
- c. Belgilari bilan
- d. Samaradorligi bilan

**196) Kriptografik himoya axborotning quyidagi xususiyatlaridan qay birini ta'minlamaydi?**

**a. Foydalanuvchanlikni**

- b. Butunlikni
- c. Maxfiylikni
- d. Autentifikatsiyani

**197) Elektron raqamli imzo tizimi**

**foydalanuvchining elektron raqami imzosini uning imzo chekishdagi maxfiy kalitini bilmasdan qalbakilashtirish imkoniyati nimalarga bog'liq?**

**a. Buning imkoni yo'q**

- b. Foydalanilgan matematik muammoga
- c. Ochiq kalit uzunligiga
- d. Imzo chekiladigan matnni konfidensialligiga

**198) Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni-bu:**

**a. Identifikatsiya**

b. Autentifikatsiya

c. Avtorizatsiya

d. Ma'murlash

**199) Sub'ektga ma'lum vakolat va resurslardan foydalanish imkoniyatini berish muolajasi- bu:**

**a. Avtorizatsiya**

b. Autentifikatsiya

c. Identifikatsiya

d. Haqiqiylikni ta'minlash

**200) Lokal simsiz tarmoqlarga tegishli texnologiyani ko'rsating?**

**a. WI-FI**

b. WI-MAX

c. GSM

d. Bluetooth

**201) Qaysi shifrlash algoritmi GSM tarmog'ida foydalaniladi?**

**a. A5/1**



- b. RC4
- c. AES
- d. RSA

## **202) Qaysi javobda elektron raqamli imzoning afzalligi noto'g'ri keltirilgan?**

- a. **Imzo chekilgan matn foydalanuvchanligini kafolatlaydi**
- b. Imzo chekilgan matn imzo qo'yilgan shaxsga tegishli yekanligini tasdiqlaydi
- c. Shaxsga imzo chekilgan matnga bog'liq majburiyatlaridan tonish imkoniyatini bermaydi
- d. Imzo chekilgan matn yaxlitligini kafolatlaydi

## **203) Tomonlar autentifikatsiyasini, uzatilayotgan ma'lumot butunligi va maxfiyligini ta'minlovchi himoya vositasi bu?**

- a. **VPN**
- b. Tarmoqlararo ekran
- c. Antivirus
- d. Router

**204) Paket filterlari turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi?**

**a. Tarmoq sathi parametrlari asosida**

- b. Kanal sathi parametrlari asosida
- c. Ilova sathi parametrlari asosida
- d. Taqdimot sathi parametrlari asosida

**205) OSI modelining qaysi sathida VPNni qurib bo'lmaydi?**

**a. Fizik sathda**

- b. Kanal sathda
- c. Tarmoq sathda
- d. Seans sathda

**206) Qaysi tarmoq himoya vositasi taqiqlangan saytlardan foydalanish imkoniyatini beradi?**

**a. VPN**

- b. Tarmoqlararo ekran
- c. Antivirus
- d. Router

**207) OSI modelining tarmoq sathiga mos parametrlarni ko'rsating?**

**a. IP manzil**

- b. MAS manzil
- c. Portlar
- d. SSL protokoli

**208) OSI modelining kanal sathiga mos parametrlarni ko'rsating?**

**a. MAS manzil**

- b. IP manzil
- c. Portlar
- d. SSL protokoli

**209) OSI modelining transport sathiga mos parametrlarni ko'rsating?**

**a. Portlar**

- b. MAS manzil
- c. IP manzil
- d. SSL protokoli

**210) Hodisalarni qayd etish quyidagilardan qaysi imkoniyatni taqdim etmaydi?**

**a. Yo'qolgan ma'lumotni tiklash imkoniyatini**

- b. Bo'lishi mumkin bo'lgan hujumni oldini olish imkoniyatini
- c. Xatolik sababini bilish imkoniyatini
- d. Holat haqida to'liq ma'lumot olish imkoniyatini

## **2-qism**

**1. Elektron axborot saqlovchilardan qayta foydalanishli ma'lumotlarni yo'q qilish usullari orasidan eng ishonchlisini aniqlang.**

**a. Formatlash**

- b. Delete buyrug'l yordamida o'chirish
- c. Shift+Delete buyrug'l yordamida o'chirish
- d. Takroriy qayta yozish

**2.  $5 \text{ XOR } 8 = ?$  Natijani hisoblang.**

**a. 13**

- b. 10
- c. 11
- d. 40

**3. Agar  $a$  – ochiq kalit,  $b$  – shaxsi kalit,  $H$  – xabar,  $X()$  – xesh funksiya bo'lsa  $\text{Sign}()$  – imzolash funksiyasi uchun asosiy parametrlariga asoslangan ko'rinishini ko'rsating.**

**a.  $\text{Sign}(X(H), a)$**

- b.  $\text{Sign}(H, a)$
- c.  $\text{Sign}(H, b)$

**d.  $\text{Sign}(X(H), b)$**

**4. Ma'lumotni to'liq qayta tiklash qachon samarali amalga oshiriladi?**

**a. Formatlash asosida ma'lumot o'chirilgan bo'lsa**

- b. Saqlagichda ma'lumot qayta yozilmagan bo'lsa
- c. Ma'lumotni o'chirish Delete buyrug'i bilan amalga oshirilgan bo'lsa
- d. Ma'lumotni o'chirish Shift+Delete buyrug'i bilan amalga oshirilgan bo'lsa

**5. .... - ushbu zaxiralashda tarmoqqa bog'lanish amalga oshiriladi. Ushbu zaxiralashda, tizim yangilanishi davomiy yangilanishni qabul qilish uchun ulanadi.**

- a. Issiq zaxiralash
- b. Ichki zaxiralash
- c. Iliq zaxiralash
- d. Sovuq zaxiralash

**6. Agar biror xesh funksiyaga kiruvchi ma'lumot uzunligi 512 bit bo'lganida, chiquvchi qiymat 128 bitga teng bo'lsa, shu funksiyaga 1024 bit ma'lumot kiritilganida chiqish biti necha bitga teng bo'ladi?**

**a. Hisoblash uchun shartlar yetarli emas**

**b. 128**

c. 64

d. 256

**7. Sotsial injeneriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan?**

**a. Biometrik autentifikatsiya**

b. Ko'z qorachig'iga asoslangan autentifikatsiya

c. Tokenga asoslangan autentifikatsiya

**d. Parolga asoslangan autentifikatsiya**

**8.  $2 \text{ XOR } 6 = ?$  Natijani hisoblang.**

**a.4**

b.6

c.8

d.12

**9. VPNning texnik yechim arxitekturasiga ko'ra turlari keltirilgan qatorni toping.**

**a. Kanal sathidagi VPN; tarmoq sathidagi VPN; seans sathidagi VPN**

b. Dasturiy ko'rinishdagi VPN; maxsus shifrlash protsessoriga ega apparat vosita ko'rinishidagi VPN

c. Marshuritizator ko'rinishidagi VPN; tarmoqlararo ko'rinishidagi VPN

d. Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN

**10.  $6 \text{ XOR } 6 = ?$  Natijani hisoblang.**

a. 0

b. 6

c. 12

d. 36

**11. Parolga xos bo'lmagan xususiyatni ko'rsating.**

a. Klaviatura orqali barcha kiritiluvchi qiymatlarni qabul qiladi

b. PIN kodni parolni xususiy holati sifatida qarash mumkin

c. Ixtiyoriy uzunlikda bo'lishi mumkin

d. Faqat pechat qilinuvchi belgilarni qabul qiladi

**12. Tarmoqlararo ekran vositasi bajarilishiga ko'ra qanday turlarga bo'linadi?**

a. **Paket filterlari – tarmoq sathida ishlaydi, ekspert paketi**

filterlari – transport sathida ishlaydi; ilova proksilari – ilova sathida ishlaydi

b. Yagona tarmoq himoyasi sxemasi; himoyalangan yopiq va himoyalanganmagan ochiq tarmoq segmentli sxema; bo'lingan himoyalangan yopiq va ochiq segmentli tarmoq sxemasi



- c. Apparat-dasturiy: Dasturiy
- d. Protokol holatini nazoratlash: vositachi yordamida(proksi)

### **13. GSM tarmog'ida ovozli so'zlashuvlarni shifrlash algoritmi bu?**

**a. RSA**

- b. A5/1
- c. ΓOCT
- d. DES

### **14. Xavfsizlik siyosati xususiyatlari keltirilgan qatorni ko'rsating.**

**a. Tushunarli bo'lishi, amaliy bo'lishi**

- b. Barcha javoblar to'g'ri
- c. Qisqa va aniq foydalanuvchan bo'lishi
- d. Iqtisodiy asoslangan bo'lishi

### **15. Biba modelida birinchi ob'ektning ishonchlilik darajasi I(01) ga va ikkinchi ob'ektning ishonchlilik darajasi I(02) ga teng bo'lsa, ushbu ikkita ob'ektdan iborat bo'lgan uchinchi ob'ektning**

**ishonchlilik darajasi nimaga teng? Bu yerda  $I(01) > I(02)$ .**

**a.  $I(02)$**

- b. Berilgan shartlar yetarli emas
- c.  $I(01)$  va  $I(02)$  ga bog'liq emas
- d.  $I(01)$

**16. Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi?**

**a. Antivirus**

- b. Router
- c. Tarmoqlararo ekran
- d. Virtual himoyalangan tarmoq

**17. Elektron raqamli imzo keltirilganlardan qaysi xususiyatni ta'minlamaydi?**

**a. Yaxlitlik**

- b. Qalbakilashtirishdan himoya
- c. Konfidensiallik
- d. Rad etishdan himoya

**18. Zudlik bilan chora ko'rish talab etilmasada, qisqa vaqtda qarshi harakatlarni qo'llash zarur; Riskni yetarlicha past darajagacha tushurish uchun imkoni boricha nazorati amalga oshirish kerak. Mazkur harakatlar riskning qaysi darajasi uchun?**

- a. Quyi**
- b. Barcha
- c. Yuqori
- d. O'rta

**19. Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo'shimcha apparat va dasturiy vositani talab qiladi?**

- a. USB disklar**
- b. Ko'chma qattiq disklar
- c. CD/DVD disklar
- d. Lentali disklar

**20. Eng zaif simsiz tarmoq protokolini ko'rsating.**

- a) WPA3**
- b) WEP

c) WPA2

d) WPA

**21. Parolga “tuz”ni qo’shib xeshlashdan maqsad?**

**a) Tahdidchi ishini oshirish**

b) Murakkab parol hosil qilish

c) Yana bir maxfiy parametr kiritish

d) Murakkab xesh qiymat qiymat hosil qilish

**22. (Bob-), (Alisa,rw), (Sem,rw), (buxgalteriyaga oid dastur,rw). Ushbu qoida quyidagilardan qaysi biriga tegishli?**

**a) Biba modeli**

b) Imtiyozlar ro’yhati yoki C-list

c) Foydalanishni boshqarish ro’yhati yoki ACL

d) Foydalanishni boshqarish matritsasi

**23. Jumlani to’ldiring. .... - muhim bo’lgan avborot nusxalash yoki saqlash jarayoni bo’lib, bu ma’lumot yo’qolgan vaqtda qayta tiklash imkoniyatini beradi.**

**a) VPN**

- b) Kriptografik himoya
- c) Ma'lumotlarni zaxira nusxalash
- d) Tarmoqlararo ekran

**24. Sub'ekt.lavozimi=Vrach & muhit.vaqt >= 8:00  
& muhit.vaqt <= 18:00. Ushbu keltirilgan shart  
qaysi foydalanishni boshqarish usuliga tegishli?**

**a) Rolga asoslangan foydalanishni boshqarish**

- b) Mandatli foydalanishni boshqarish
- c) Attributga asoslangan foydalanishni boshqarish
- d) Diskretsiya foydalanishni boshqarish

**25. Trafik orqali axborotni to'plashga harakat  
qilish razvedka hujumlarining qaysi turida amalga  
oshiriladi?**

**a) Lug'atga asoslangan**

- b) Passiv
- c) DNS izi
- d) Aktiv

**26. Modul arifmetikasida mod7 bo'yicha 4 soniga teskari bo'lgan sonni toping?**

**a)  $\frac{1}{4}$**

b) 2

c) 4

d) 7

**27. A5/1 shifrlash algoritmida registrlar siljiganidan keying holat:  $x_{18}=0$ ,  $y_{21}=1$  va  $z_{22}=1$  ga teng bo'lsa, hosil bo'lgan psevdotasodifiy qiymatni ko'rsating.**

**a) 0**

b) 11

c) 1

d) 110

**28. Zaxiralashni amalga oshirishda inson ishtirokini talab etadi; Tabiiy-ofatlarga yoki o'g'irlashga moyil. Ushbu xususiyat qaysi zaxira nusxalash manziliga tegishli?**

**a) Bulutli tizmda zaxiralash**

- b) Barcha javoblar to'g'ri
- c) Tashqi (offsite) zaxiralash
- d) Ichki (onsite) zaxiralash

## **29. Resurslardan foydalanish usuliga ko'ra kompyuter viruslari qanday turlarga bo'linadi?**

**a) Shifrlangan, shifrlanmagan va polimorf**

- b) Dasturiy, yuklanuvchi, makroviruslar va ko'p platformali
- c) Resident va norezident
- d) Virus-parazitlar va virus-chervlar

## **30. Risk ta'sirini kamaytirish uchun profilaktika choralarini ko'rish zarur. Mazkur harakatlar riskning qaysi darajasi uchun?**

**a) Barcha**

- b) Quyi
- c) O'rta
- d) Yuqori

## **31. TCP/IP modelidagi kanal sathi OSI modelidagi qaysi sathlarga mos keladi?**

**a) Tarmoq va kanal**

- b) Kanal
- c) Fizik va kanal
- d) Fizik

**32. “Kompilyator foydalanuvchining imtiyoziga ko’ra ish ko’rish o’rniga o’zining imtiyoziga asosan ish ko’rishi” klassik xavfsizlik sohasida nima deb yuritiladi?**

- a) Donadorlik muammosi**
- b) Klassifikatsiyalashdagi muammo
- c) Cheklanishdagi muammo
- d) Tartibsiz yordamchi muammosi

**33.  $2 \text{ XOR } 4 = ?$  Natijani hisoblang.**

- a) 6**
- b) 4
- c) 2
- d) 8

**34.  $5 \text{ XOR } 8 = ?$  Natijani hisoblang.**

- a) 10**
- b) 13**



c) 40

d) 12

**35. Markaziy xab yoki tugun orqali tarmoqni markazlashgan holda boshqarish qaysi tarmoq topologiyasida amalga oshiriladi?**

a) Mesh

b) Xalqa

c) Shina

d) Yulduz

**36. Yaratishda psevdotasofiy sonlar generatoriga asoslanuvchi kriptografik shifrlash usuli bu?**

a) Ochiq kalitli

b) Assimmetrik

c) Simmetrik blokli

d) Simmetrik oqimli

**37.  $4 \text{ XOR } 4 = ?$  Natijani hisoblang.**

a) 0

b) 8

c) 16

d) 4

**38. Elektron raqamli imzo muolajalarini ko'rsating.**

**a) Imzoni shakllantirish va xeshlash**

b) Imzoni xeshlash va xesh matni deshifrlash

c) Shifrlash va deshifrlash

d) Imzoni shakllantirish va imzoni tekshirish

**39. Foydalanuvchining tizimga muvaffaqiyatli urinishi Windows OT da qanday audit hodisasi sifatida qayd etiladi?**

**a) Muvaffaqiyatsiz audit**

b) Ogohlantirish

c) Xatolik

d) Muvaffaqiyatli audit

**40. Ushbu hujumda foydalanuvchilarning akkauntlari bloklangani va kredit karta ma'lumotlari blokdan chiqarilishi kerakli to'g'risidagi ma'lumot foydalanuvchi electron pochta lariga yuboriladi. Gap qaysi ijtimoiy injeneriya turi haqida bormoqda?**

**a) Phishing**

b) Spoofing

c) Protexting

d) Barcha javoblar to'g'ri

**41. Ma'lumotni zaxira nusxalash nima uchun potensial tahdidlarni paydo bo'lish ehtimolini oshiradi?**

**a) Tahdidchi uchun nishon ko'payadi**

b) Ma'lumot yo'qolgan taqdirda ham tiklash imkoniyati mavjud bo'ladi

c) Saqlanuvchi ma'lumot hajmi ortadi

d) Ma'lumotni butunligi ta'minlanadi

**42. Manbaga zarar keltiradigan ichki va tashqi zaiflik ta'sirida tahdid qilish ehtimoli bu?**

**a) Hujum**

b) Zaiflik

c) Risk

d) Tahdid

**43. RSA algoritmda ochiq kalit  $e=5$ ,  $N=35$  ga teng bo'lsa,  $M=3$  ga teng ochiq matnni shifrlash natijasini ko'rsating.**

**A) 35**

B) 7

C) 5

**D) 33**

**44. RAID 3 texnologiyasing vazifasi –**

**A) Diskni navbatlanishi va xatolikni nazoratlash**

B) Bloklarni navbatlash va akslantirish

C) Diskni navbatlanishi

D) Diskni akslantirish

**45. RSA algoritmda  $p=3$ ,  $q=11$  bo'lsa,  $N$  sonidan kichik va u bilan o'zaro tub bo'lgan sonlar miqdorini ko'rsating.**

**a) 14**

b) 33

c) 20

d) 12

**46. Resursni va harakatni kim bajarayotgani to'g'risidagi holatlar "AGAR, U HOLDA" dan tashkil topgan qoidalarga asoslanadi. Gap qaysi foydalanishni boshqarish usuli haqida bormoqda?**

**A) DAC**

B) MAC

C) RBAC

D) ABAC

**47. Ichki yoki tashqi majburiyatlar natijasida tahdid yoki hodisalarni yuzaga kelishi, yo'qotilishi yoki boshqa salbiy ta'sir ko'rsatishi mumkin bo'lgan voqea bu?**

**A) Risk**

B) Hujum

C) Tahdid

D) Zaiflik

**48. Jumlani to'ldiring. Tarmoqlararo ekranning vazifasi ...**

**A) Tarmoq hujumlarini aniqlash**

B) Tarmoqdagi xabarlar oqimini uzish va ulash

C) Ishonchli va ishonchsiz tarmoqlar orasida ma'lumotlarga kirishni boshqarish

D) Trafikni taqiqlash

**49. Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan?**

**A) Apparat nazoratlash**

B) Ma'muriy nazoratlash

C) Texnik nazoratlash

D) Fizik nazoratlash

**50. RSA algoritmidagi  $p=7$ ,  $q=5$  bo'lsa,  $N$  sonidan kichik va  $u$  bilan o'zaro tub bo'lgan sonlar miqdorini ko'rsating.**

**A) 24**

- B) 35
- C) 12
- D) 60

**51. Foydalanishni boshqarish matritsasi ustunlar bo'yicha bo'linsa ... hosil bo'ladi.**

**A) Foydalanishni boshqarish ro'yhati yoki ACL**

- B) Foydalanishni boshqarish matritsasi
- C) Imtiyozlar ro'yhati yoki C-list
- D) Biba modeli

**52. Faraz qilaylik tizimdagi barcha fayllarni xeshlab, xesh qiymatlari xavfsiz manzilga saqlangan bo'lsin. U holda vaqti-vaqti bilan ushbu faylning xesh qiymatlari qaytadan xeshlanadi va dastlabki holatdagilari bilan taqqoslanadi. Agar faylning bir yoki bir nechta bitlari oz'garishga uchragan bo'lsa, u holda xesh bir-biriga mos kelmaydi va natijada uni virus tomonidan zararlangan deb qarash mumkin. Bu zararli**

**dasturiy vositalarmi aniqlashning qaysi usuliga misol bo'ladi?**

**A) Anomaliyaga asoslangan**

- B) Signaturaga asoslangan
- C) O'zgarishni aniqlashga asoslangan
- D) Barchasiga

**53. Parollarni saqlashda nega shifrlashning o'rniga xeshlash amalidan foydalaniladi?**

**A) Shifrlash algoritmlari xavfsiz emas**

- B) Shifrlash algoritmlari tezkor emas
- C) Xesh funksiyalari xavfsiz
- D) Shifrlash kalitini saqlash zaruriyati mavjud

**54. Modul arifmetikasida mod7 bo'yicha 5 soniga teskari bo'lgan sonni toping?**

**A) 3**

- B) 35
- C) 2



D) 5/7

**55. Voqea sodir bo'lish ehtimoli va ushbu hodisaning axborot texnologiyalari aktivlariga ta'siri bu?**

**A) Hujum**

B) Tahdid

C) Zaiflik

D) Risk

**56. Kriptografiya so'ziga berilgan to'g'ri tavsifni toping?**

**A) Maxfiy shifrlarni yaratish va buzish fani va san'ati**

B) Maxfiy shifrlarni yaratish fani va san'ati

C) Axborotni himoyalash fani va san'ati

D) Maxfiy shifrlarni buzish fani va san'ati

**57. Asosiy maqsad ma'lumotni maxfiyligini ta'minlash bo'lgan jarayonni ko'rsating?**

**A) Dekodlash**

- B) Kodlash
- C) Shifrlash
- D) Deshifrlash

**58. Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting.**

**A) Almashib bo'lmashlik**

- B) Doimo esda saqlash zaruriyati
- C) Doimo xavfsiz saqlab olib yurish zaruriyati
- D) Qalbakilashtirish muammosi mavjudligi

**59. Agar  $d$  – ochiq kalit,  $e$  – shaxsi kalit,  $X$  – xabar,  $H()$  – xesh funksiya bo'lsa  $Sign()$  – imzolash funksiyasi uchun asosiy parametrlariga asoslangan ko'rinishini ko'rsating.**

**A)  $Sign(X, d)$**

- B)  $Sign(X, e)$
- C)  $Sign(H(X), d)$
- D)  $Sign(H(X), e)$

**60. RSA algoritmda  $p=5$ ,  $q=11$  bo'lsa,  $N$  sonidan kichik va  $u$  bilan o'zaro tub bo'lgan sonlar miqdorini ko'rsating.**

**A) 55**

B) 10

C) 11

D) 40

**61. Paydo bo'lishi tasodifiy, qasddan yoki boshqa harakatning ta'sirida bo'lishi mumkin bo'lgan hodisa bu?**

**A) Tahdid**

B) Aktiv

C) Hujum

D) Zaiflik

**62. Risklarga qarshi zudlikda chora ko'rish zarur; riskni yetarlicha past darajagacha tushirish uchun**

**nazoratlash vositalarini aniqlash va o'rnatish kerak.**

**Mazkur harakatlar riskning qaysi darajasi uchun?**

- A) O'rta
- B) Yuqori
- C) Quyi
- D) Barcha

**63. Ushbu hujumda qurbonni shubhalanmasligi uchun tegishli tayyorgarlik ko'riladi: tug'ilgan kun, INN, passport raqami yoki hisob raqamining oxirgi belgilari kabi ma'lumotlar topiladi. Gap qaysi ijtimoiy injineriya turi haqida bormoqda?**

**A) Barcha javoblar to'g'ri**

- B) Protexing
- C) Phishing
- D) Spoofing

**64. Turli xil psixologik usullar va firibgarlik amaliyoting turlari bo'lib, uning maqsadi firibgarlik**

**yo'li bilan shaxs to'g'risida maxfiy ma'lumotlarni olishdan iborat. Gap nima haqida bormoqda?**

**A) Kibernetika**

B) Kiberxavfsizlik

C) Ijtimoiy injeneriya

D) Kiberjinoyatlar

**65. A5/1 oqimli shifrlash algoritmida maj(1,1,1) ga bo'lsa, qaysi registorlar siljiydi?**

**A) Y**

B) X,Y,Z

C) X,Y

D) X,Z

**66. Ochiq kalitli kriptotizimda ma'lumotga imzo qo'yish qaysi kalit yordamida amalga oshiriladi?**

**A) Yuboruvchining ochiq kaliti**

B) Qabul qiluvchining ochiq kaliti

C) Yuboruvchining shaxsiy kaliti

D) Qabul qiluvchining shaxsiy kaliti

**67. Modul arifmetikasida mod11 bo'yicha 3 soniga teskari bo'lgan sonni toping?**

**A) 5**

B)  $1/11$

C) 4

D)  $1/3$

**68. A5/1 algoritmidagi Y registri uzunligi nechiga teng?**

**A) 21**

B) 22

C) 23

D) 19

**69. RSA algoritmidagi ochiq va shaxsiy kalitlar uchun qanday munosabat o'rinli?**

**A) Ochiq va shaxsiy kalitlar  $\text{mod}(p \cdot q)$  bo'yicha o'zaro teskari**

- B) Ochiq va shaxsiy kalitlar uchun biror munosabat o'rinli emas
- C) Ochiq va shaxsiy kalitlar modN bo'yicha o'zaro teskari
- D) Ochiq va shaxsiy kalitlar mod $\phi(N)$  bo'yicha o'zaro teskari

**70. Eng kam vaqtda ma'lumotni tiklash imkoniyatiga ega usul bu?**

- A) Differensial zaxiralash**
- B) O'sib boruvchi zaxiralash
- C) To'liq zaxiralash
- D) Ichki zaxiralash

**71. Qurbon kompyuteridagi ma'lumotni shifrlab, uni deshifrlash uchun to'lovni amalga oshirishni talab qiluvchi zararli dastur bu-?**

- A) Rootkits**
- B) Mantiqiy bombalar
- C) Spyware
- D) Ransomware

## 72. Tarmoqlararo ekran vositasi OSI modeling funksional sathlari bo'yicha qanday turlarga bo'linadi?

A) Paket filterlari – tarmoq sathida ishlaydi; ekspert paketi filterlari – transport sathida ishlaydi; ilova proksilari – ilova sathida ishlaydi

B) Protokl holatini nazoratlash; vositachi yordamida nazoratlash (proksi)

C) Apparat-dasturiy; dasturiy

D) Yagona tarmoq himoyasi sxemasi; himoyalangan yopiq va himoyalanmagan ochiq tarmoq segmentli sxema; bo'lingan himoyalangan yopiq va ochiq segmentli tarmoq sxemasi

## 73. Ochiq matn qismlarini takroriy shifrllovchi algoritmlar bu –

A) Blokli shifrlar

B) Ochiq kalitli shifrlar

C) Asimmetrik shifrlar

D) Oqimli shifrlash



**74. Ma'lumot shifrlansa, natijasi .... bo'ladi.**

**A) No'malum**

B) Ochiq matn

C) Kod

D) Shifrmtn

**75. Tarmoqdagi barcha tugunlarni o'zaro bog'laydi.**

**Gap qaysi topologiya haqida bormoqda?**

**A) Halqa**

B) Yulduz

C) Shina

D) Daraxt

**76. Agar simmetrik oqimli shifrlash algoritmida**

**kiritilgan ochiq matn uzunligi 256 bitga teng bo'lsa,  
shifrmtn uzunligi necha bit bo'ladi?**

**A) 128**

B) 256

C) 4

D) 64

**77. Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu?**

**A) Identifikatsiya**

B) Autentifikatsiya

C) Ro'yxatga olish

D) Avtorizatsiya

**78. Parollar 10 xonali uzunlikka va har bir xonasi uchun 16ta turli belgilar bo'lishi mumkin bo'lgan jami parollar soni nechta?**

**A) 26**

B) 160

C)  $10^{16}$

D)  $16^{10}$

**79. Shaxsni kimdir deb davo qilish jarayoni bu?**

**A) Ruxsatlarni nazoratlash**

B) Avtorizatsiya

- C) Autentifikatsiya
- D) Identifikatsiya

**80. VPNni OSI modelining “ishchi sathlari” ga ko’ra turlari keltirilgan qatorni aniqlang?**

**A) Kanal sathidagi vpn; tarmoq sathidagi vpn; seans sathidagi vpn**

- B) Dasturiy ko’rinishdagi vpn; maxsus shifrlash protsessoriga ega apparat vosita ko’rinishidagi vpn
- C) Korporativ tarmoq ichidagi vpn; masofadan foydalaniluvchi vpn; korporativ tarmoqlararo vpn
- D) Marshuritizator ko’rinishidagi vpn; tarmoqlararo ekran ko’rinishidagi vpn

**81. Asosiy fayl tizimining ustida joylashgan kriptografik fayl tizimidan foydalaniladi. Gap qaysi shifrlash usuli xususida bormoqda?**

**A) Dasturiy shifrlash**

- B) Faylni shifrlash
- C) Apparat shifrlash

D) Diskni shifrlash

**82. Yo'q qilish usullari orasidan ekologik jihatdan ma'qullanmaydigan va maxsus joy talab qiladigan usul qaysi?**

**A) Ko'mish**

B) Yoqish

C) Kimyoviy ishlov berish

D) Maydalash

**83. Qaysi akslantirishda ochiq matndagi belgilarning takrorlanish chastotasi shifrmatndagi belgilarda ham bir xil bo'ladi?**

**A) Bir alifboli o'rniga qo'yish**

B) Gammalash

C) Qo'shish

D) O'rin almashtirish

**84. Blokli simmetrik shifrlashda shifrmatndagi bir bitning o'zgarishi deshifrlangan matndagi necha bitning o'zgarishiga olib keladi?**

**A) Buni aniqlash imkonsiz**

B) 1

C) Barchasiga

D) Kamida bir blokiga

**85. [www.PayPai.com](http://www.PayPai.com) manzili [www.PayPal.com](http://www.PayPal.com) manzili sifatida yuboriladi. Bu qaysi turdagi hujumga misol bo'ladi?**

**A) Protexting**

B) Phishing

C) Spoofing

D) Barcha javoblar to'g'ri

**86. Zaxira nusxalash manzillarini ko'rsating.**

**A) To'liq, differensial va o'sib boruvchi zaxiralash**

B) Barcha javoblar to'g'ri

- C) Issiq, sovuq va iliq zaxiralash
- D) Ichki, tashqi va bulutda zaxiralash

**87. AGAR talabgor boshqaruvchi bo'lsa, U HOLDA maxfiy ma'lumotni o'qish/yozish huquqi berilsin. Bu qaysi foydalanishni boshqarish usuliga misol bo'ladi?**

**A) DAC**

- B) RBAC
- C) MAC
- D) ABAC

**88. A5/1 oqimli shifrlash algoritmining bir siklda kamida nechta registr siljiydi?**

**A) 3**

- B) 1
- C) 0
- D) 2

**89. Bir-biriga osonlik bilan ma'lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi bu?**

**A) Tarmoq topologiyasi**

- B) Kompyuter tarmog'i
- C) Kompyuter topologiyasi
- D) Tarmoq arxitekturasini

**90. Subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim etish jarayoni bu?**

**A) Avtorizatsiya**

- B) Identifikatsiya
- C) Ruxsatlarni nazoratlash
- D) Autentifikatsiya

**91. Foydalanishni boshqarishning qaysi usulida asosiy g'oya tizimning ishlash logikasini tashkilotdagi kadrlar vazifasiga yaqinlashtirishga harakat qilinadi?**

A) DAC

B) RBAC

C) MAC

D) ABAC

**92. Yong'inga qarshi kurashishning aktiv usuli to'g'ri ko'rsatilgan javobni toping.**

A) Minimal darajada yonuvchan materiallardan foydalanish, qo'shimcha etaj va xonalar qurish

B) Binoga istiqomat qiluvchilarni yong'in sodir bo'lganda qilinishi zarur bo'lgan ishlar bilan tanishtirish

C) Yetarli sondagi qo'shimcha chiqish yo'llarini mavjudligi

D) Tutunni aniqlovchilar, alangani aniqlovchilar va issiqlikni aniqlovchilar

**93. A5/1 shifrlash algoritmda registrlar siljiganidan keying holat:  $x_{18}=1$ ,  $y_{21}=1$  va  $z_{22}=1$  ga teng bo'lsa, hosil bo'lgan psevdotasodifiy qiymatni ko'rsating.**

A) 0



- B) 11
- C) 111
- D) 1

**94. Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating.**

**A) Parollar lug'atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydalanish asosida hujum**

- B) Parollar lug'atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararki dasturlardan foydalanish asosida hujum
- C) Fizik o'g'irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar
- D) Fizik o'g'irlash, yelka orqali qarash hujumi, zararli dasturlardan foydalanishga asoslangan hujumlar

**95. Seans sathidagi VPN qaysi protocol asosida quriladi?**

**A) IPsec**

B) PPTP

C) L2F

D) TLS

**96. RSA algoritmda  $p=7$ ,  $q=11$ ,  $e=7$  ga teng bo'lsa, shaxsiy kalitni hisoblang.**

**A) 43**

B) 7

C) 77

D) 11

**97. Qaysi himoya vositasi mavjud IP – paketni to'liq shifrlab, unga yangi IP sarlavha beradi?**

**A) Router**

B) Tarmoqlararo ekran

C) VPN

D) Antivirus

**98. Faqat simsiz tarmoqlarga xos bo'lgan zaifliklarni ko'rsating?**

**A) Zararli dasturlardan foydalanishga asoslangan hujumlarni mavjudliligi**

- B) Nazoratlanmaydigan hududni har doim mavjudligi
- C) Xizmat ko'rsatishdan voz kechish hujumini mavjudligi
- D) O'rta turgan odam hujumini mavjudligi

**99. Juda ahamiyatli emas, lekin kelajakda yuzaga kelishi mumkin bo'lgan muammolarni ko'rsatishi mumkin bo'lgan voqealar Windows OTda qanday hodisa sifatida qayd etiladi?**

**A) Axborot**

- B) Muvaffaqiyatsiz audit
- C) Ogohlantirish
- D) Xatolik

**100. Qaysi holatni normal va qaysi holatni normal bo'lmagan deb topish va ushbu ikki holat orasidagi farqni aniqlashga asoslanadi. Ushbu xususiyat zararli dasturiy vositalarni aniqlashning qaysi usuliga tegishli?**

**A) Barchasiga**

- B) Signaturaga asoslangan
- C) O'zgarishni aniqlashga asoslangan
- D) Anomaliyaga asoslangan

**101. Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo'lgan murojaatlarini chegaralash qaysi himoya vositasing vazifasi hisoblanadi?**

**A) Antivirus**

- B) Router
- C) Tarmoqlararo ekran
- D) Virtual himoyalangan tarmoq

**102. Tashqi ma'lumotlarni bazaga yuklashda qanday kengaytmali fayl formatidan foydalansa bo'ladi?**

**A) JPEG**

- B) PDF
- C) CSV

D) DOCX

**103. Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat'iy nazar muvaffaqiyatli o'rnatuvchi asos bu?**

**A) Tarmoq modeli**

B) Kompyuter tarmog'i

C) Mobil tarmoq

D) Tarmoq topologiyasi

**104. WEP, WPA, WPA2 protokollari qaysi simsiz texnologiyada ishlatilgan?**

**A) WiMax**

B) Wi-Fi

C) GSM

D) Bluetooth

**105. Zaxira nusxalash strategiyasi rejasi nimadan boshlanadi?**

**A) Mos zaxira nusxalash usulini tanlashdan**

- B) Zaxira nusxalash texnologiyasini tanlashdan
- C) Zaxira nusxalash uchun xotira qurilmasini tanlashdan
- D) Tashkilot missiyasi uchun zarur axborotni aniqlashdan

**106. Tashkilot axborot aktivlarini va binolaridan foydalanishni kuzatish, qaydlash va nazoratlashga yordam beruvchi xavfsizlik turi?**

**A) Iqtisodiy xavfsizlik**

- B) Fizik xavfsizlik
- C) Huquqiy xavfsizlik
- D) Tarmoq xavfsizligi

**107. Xavfsizlik siyosatlarining afzalliklari keltirilgan qatorni toping.**

**A) Kuchaytirilgan ma'lumot va tarmoq xavfsizligini ta'minlaydi**

- B) Qurilmalardan foydalanish va ma'lumotlar transferining monitoringlanishi va nazoratlanishini ta'minlaydi
- C) Barcha javoblar to'g'ri
- D) Risklarni kamaytiradi

**108. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to'plami bu?**

**A) Xavfsizlik doktorinasi**

B) Xavfsizlik siyosati

C) Xavfsizlik konsepsiyasi

D) Tashkilot nizomi

**109. A5/1 oqimli shifrlash algoritmida maj(1,0,1) ga bo'lsa, qaysi registrlar siljiydi?**

**A) X,Y,Z**

B) Y

C) X,Z

D) X,Y

**110. RSA algoritmida  $p=7$ ,  $q=19$  bo'lsa,  $N$  sonidan kichik va u bilan o'zaro tub bo'lgan sonlar miqdorini ko'rsating.**

**A) 133**

- B) 26
- C) 72
- D) 108

**111. A5/1 oqimli shifrlash algoritmida maj(0,1,0) ga bo'lsa, qaysi registorlar siljiydi?**

**A) X,Y,Z**

- B) Y
- C) X,Z
- D) X,Y

**112. Ochiq kalitli shifrlash algoritmida ma'lumotni shifrlab yuborish qaysi kalit yordamida amalga oshiriladi?**

**A) Qabul qiluvchining shaxsiy kaliti**

- B) Qabul qiluvchining ochiq kaliti
- C) Yuboruvchining shaxsiy kaliti
- D) Yuboruvchining ochiq kaliti



**113. Yong'inga qarshi tizimlarni aktiv chora turiga quyidagilardan qaysilari kiradi.**

**A) Yong'inga aloqador tizimlarni to'g'ri madadlanganligi**

B) Yong'inni aniqlash va bartaraf etish tizimi

C) Minimal darajada yonuvchan materiallardan foydalanish

D) Yetarlicha miqdorda qo'shimcha chiqish yo'llarini mavjudligi

**114. Modul arifmetikasida mod11 bo'yicha 5 soniga teskari bo'lgan sonni toping?**

**A) 9**

B) 4

C)  $1/11$

D)  $1/5$

**115. Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzatib boruvchi zararli dastur turi bu?**

**A) Backdoors**

- B) Adware
- C) Spyware
- D) Troyan otlari

**116. Kompyuter viruslarini tarqalish usullarini ko'rsating.**

**A) Ma'lumot saqlovchilari, internetdan yuklab olish va skaner qurilmalari orqali**

- B) Barcha javoblar to'g'ri
- C) Ma'lumot saqlovchilari, internetdan yuklab olish va electron pochta orqali
- D) Printer qurilmasi, internetdan yuklab olish va electron pochta orqali

**117. Riskning qaysi darajasida risk ta'sirini kamaytirish uchun profilaktika choralarini ko'rish talab etiladi?**

**A) Quyi**

- B) Yuqori
- C) Barcha darajalarda

D) O'rta

**118. Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalaniladi?**

**A) Apparat**

B) Dasturiy

C) Simmetrik

D) Ochiq kalitli

**119. RSA algoritmda ochiq kalit  $e=5$   $n=35$  ga teng bo'lsa  $M=2$  ga teng ochiq matnni shifrlash natijasini ko'rsating?**

**A) 35**

B) 7

C) 5

D) 32

**120. Modul arifmetikasida mod5 bo'yicha 4 soniga teskari bo'lgan sonni toping?**

**A) 20**

B) 1

C) 4

D) 4/5

**121. A5/1 shifrlash algoritmida registrlar siljiganidan keying holat:  $x_{18}=0$ ,  $y_{21}=0$  va  $z_{22}=1$  ga teng bo'lsa, hosil bo'lgan psevdotasodifiy qiymatni ko'rsating.**

**A) 100**

B) 0

C) 1

D) 10

**122. Simsiz lokal tarmoq texnologiyasini ko'rsating.**

**A) Ethernet**

B) Wi-Fi

C) WiMax

D) Bluetooth

**123. Parollar 6 xonali uzunlikka va har bir xonasi uchun 32 ta turli belgilar bo'lishi mumkin bo'lgan jami parollar soni nechta?**

**A)  $6^{32}$**

B)  $32!$

C)  $32^6$

D)  $6!$

**124. Har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo'shilsa ....**

**A) Hujum paydo bo'ladi**

B) Risk paydo bo'ladi

C) Aktiv paydo bo'ladi

D) Tahdid paydo bo'ladi

**125. Faqat ma'lumotga nisbatan o'zgarish yuz berganda zaxiralashni amalga oshiruvchi usuli?**

**A) Differensial zaxiralash**

- B) To'liq zaxiralash
- C) O'sib boruvchi zaxiralash
- D) Ichki zaxiralash

**126. Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas.**

**A) Turli kirishlar turli chiqishlarni akslantirishi**

- B) Kolliziyaga bardoshli bo'lishi
- C) Amalga oshirishdagi yuqori tezkorlik
- D) Bir tomonlama funksiya bo'lmasligi kerak

**127. Ob'yektning eng cheklangan imtiyoz turini aniqlang.**

**A) Private**

- B) Protected
- C) Static
- D) Public

**128. Biror mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu?**

**A) Virus**

- B) Adware
- C) Mantiqiy bombalar
- D) Backdoors

**129. Quyidagi atamalardan qaysi biri faqat simmetrik blokli shifrlarga xos?**

**A) Blok uzunligi**

- B) Kalit uzunligi
- C) Kodlash jadvali
- D) Ochiq kalit

**130. Axborotni qaysi xususiyatlari ochiq kalitli shifrlar yordamida ta'minlanadi?**

**A) Foydalanuvchanlik va konfidensiallik**

- B) Konfidensiallik, butunlik va foydalanuvchanlik
- C) Konfidensiallik
- D) Butunlik va foydalanuvchanlik

**131. Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi?**

**A) Antivirus**

B) Router

C) Tarmoqlararo ekran

D) Virtual himoyalangan tarmoq

**132. RSA algoritmda  $p=5$   $q=11$   $e=7$  ga teng bo'lsa, shaxsiy kalitni hisoblang.**

**A) 23**

B) 35

C) 24

D) 7

**133. Himoya mexanizmini aylanib o'tib tizimga ruxsatsi kirish imkonini beruvchi zarali dastur bu?**

**A) Trojan otlari**



- B) Adware
- C) Spyware
- D) Backdoors

**134. Legitimate code**

**If hour is 7 p.m:**

**crash\_computer()**

**legitimate code**

**Ushbu mantiqiy kod qaysi zararli dasturiy vositaga tegishli?**

**A) Adware**

- B) Mantiqiy bomba
- C) Virus
- D) Backdoors

**135. Diskdagi barcha ma'lumotlarni ( master boot record, (MBR) bilan) yoki MBRsiz shifrlashni amalga oshiradi. Gap qaysi shifrlash usuli haqida bormoqda?**

**A) Apparat shifrlash**

B) Dasturiy shifrlash

C) Faylni shifrlash

D) Diskni shifrlash

**136. “Single-pair shortest path problem” ushbu atama nimani anglatadi?**

**ghA)Ikkita tugun orasidagi eng qisqa masofani aniqlash masalasi**

B) Berilgan tugundan barcha tugunlarga bo'lgan qisqa yo'llarni aniqlash masalasi

C) Berilgan punktga yetib borishning qisqaroq yo'lini aniqlash masalasi

D) 3 ta tugun orasidagi eng qisqa masofani aniqlash masalasi

**137. Tarmoqdagi kompyuterlarga kabel orqali ulangan markaziy xabdan (tugun) iborat topologiya nima?**

**A) Shina**

B) Daraxt

C) Yulduz

D) Halqa

**138. Paketlarni snifferlash, portlarni skanerlash, ping buyru'gini yuborish qanday hujum turiga misol bo'ladi?**

**A) Zararli hujumlar**

B) Razvedka hujumlari

C) Xizmatdan voz kechishga undash hujumlari

D) Kirish hujumlari

**139. Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi shifrlar bu –**

**A) Ochiq kalitli shifrlar**

B) Xesh funksiyalar

C) Bir xil kalitli shifrlar

D) Simmetrik shifrlar

**140. Har bir obyekt uchun foydalanish ruxsatini belgilash o'rniga, rol uchun obyektlardan**

**foydalanish ruxsatini ko'rsatish amalga oshiriladi.  
Gap qaysi foydalanishni boshqarish usuli haqida  
bormoqda?**

**A) MAC**

B) ABAC

C) RBAC

D) DAC

**141. Biba modelida axborotni qaysi xususiyatini  
ta'minlashni maqsad qiladi?**

**A) Konfidensiallik**

B) Butunlik

C) Foydalanuvchanlik

D) Maxfiylik

**142. 2 lik sanoq tizimida 11011 soniga 11010  
sonini 2 modul bo'yicha qo'shing?**

**A) 11111**

B) 01100

C) 10000

D) 00001

**143. Quyidagi muammolardan qaysi biri simmetrik kriptotizimlarga xos.**

**A) Foydalanuvchilar tomonidan maqbul ko'rilmasligi**

B) Kalitlarni esda saqlash murakkabligi

C) Kalitni taqsimlash zaruriyati

D) Shifrlash jarayonining ko'p vaqt olishi

**144. Ma'lumotni yo'qotish yoki funksionallikni yo'qotish kabi muhim muammoni ko'rsatadigan voqealar windows OT da qanday hodisa sifatida qayd etiladi?**

**A) Xatolik**

B) Ogohlantirish

C) Muvaffaqiyatsiz audit

D) Axborot

**145. Mijozlar, foydalanuvchilar va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinuvchi hujum bu?**

**A) Spufing hujumi**

B) Razvedka hujumi

C) Kirish hujumi

D) Xizmatlardan voz kechishga undash hujumi

**146. Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko'rsating.**

**A) Ochiq kalitli shifrlar**

B) Simmetrik shifrlar

C) Oqimli shifrlar

D) Blokli shifrlar

**147. Jumlani to'ldiring. Simli va simsiz tarmoqlar orasidagi asosiy farq ...**

**A) Tarmoq chetki nuqtalari orasidagi xududning kengligi**

B) Himoyani amalga oshirish imkoniyati yo'qligi

- C) Himoya vositalarining chegaralanganligi
- D) Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlanmaydigan xudud mavjudligi

#### **148. ERI da rad etish jarayoni - ...**

**A) Foydalanuvchi (B) qabul qilib olingan ma'lumotni o'zgartirib, shu o'zgartirilgan ma'lumotni foydalanuvchi (A) yubordi deb ta'kidlaydi**

- B) (A) va (B) foydalanuvchilarning o'zaro aloqa tarmog'iga uchinchi bir (V) foydalanuvchi noqonuniy tarzda bog'lanib, ularning o'zaro uzatayotgan ma'lumotlarini o'zgartirgan holda deyarli uzluksiz uzatib turadi
- C) Foydalanuvchi (A) foydalanuvchi (B) ga haqiqatdan ham ma'lumot jo'natgan bo'lib, uzatilgan ma'lumotni rad etishi mumkin
- D) Foydalanuvchi (B) ning o'zi ma'lumot tayyorlab, bu soxta ma'lumotni foydalanuvchi (A) yubordi deb da'vo qiladi

#### **149. Eng kam xarajatli zaxira nusxalash manzilini ko'rsating.**

**A) O'sib boruvchi zaxiralash**

- B) Bulutda zaxiralash
- C) Ichki zaxiralash
- D) Tashqi zaxiralash

**150. Jumlani to'ldiring. Ma'lumotni uzatishda kriptografik himoya .....**

- A) Foydalanuvchanlik va butunlikni ta'minlaydi**
- B) Konfidensiallik va foydalanuvchanlikni ta'minlaydi
- C) Konfidensiallik va butunlikni ta'minlaydi
- D) Konfidensiallik ta'minlaydi

**151. Bell-Lapadula modelida birinchi ob'ektning xavfsizlik darajasi  $L(01)$  ga, ikkinchi ob'ektning xavfsizlik darajasi  $L(02)$  ga va uchinchi ob'ektning xavfsizlik darajasi  $L(03)$  teng bo'lsa, u holda uchta ob'ektdan iborat bo'lgan bo'lgan to'rtinchi ob'ektning xavfsizlik darajasi nimaga teng bo'ladi? Bu yerda  $L(01) < L(02) < L(03)$**

- A)  $L(03)$**
- B)  $L(02)$



- C) L(01)
- D) Berilgan shartlar yetarli emas

**152. Qaysi himoya vositasi yetkazilgan axborotning butunligini tekshiradi?**

- A) Router**
- B) Virtual Private Network
- C) Tarmoqlararo ekran
- D) Antivirus

**153. Foydalanuvchini haqiqiyligini tekshirish jarayoni bu?**

- A) Identifikatsiya**
- B) Avtorizatsiya
- C) Autentifikatsiya
- D) Ro'yxatga olish

**154. Faqat foydalanishni boshqarish usullari keltirilgan javobni ko'rsating?**

- A) DAC, MAC**

- B) ABAC, RSA
- C) RBAC, A5/1
- D) DAC, RSA

**155. Belgilangan sharoitlarda tahdidning manbalarga potensial zarar yetkazilishini kutish bu?**

**A) Risk**

- B) Tahdid
- C) Zaiflik
- D) Hujum

**156. Quyidagilardan qaysi biri tarmoq xavfsizligi muammolariga sabab bo'lmaydi?**

**A) Tug'ma texnologiya zaifligi**

- B) Routerlardan foydalanmaslik
- C) Tarmoqni xavfsiz bo'lmagan tarzda va zaif loyihalash
- D) Qurilma yoki dasturiy vositani noto'g'ri sozlanish

**157. Tarmoqning tuzilishini aniqlab, tarmoqning mantiqiy va fizik joylashuvini hisoblaydi. Gap nima haqida bormoqda?**

**A) Arxitektura**

**B) Topologiya**

C) Protokol

D) Model

**158. Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi?**

**A) Ochiq kalit**

**B) Dasturiy**

C) Simmetrik

D) Apparat

**159. Tarmoq sathidagi VPN qaysi protokol asosida quriladi?**

**A) L2F**

B) PPTP

C) TLS

D) IPSec

**160. Qanday tahdidlar passiv hisoblanadi?**

**A) Axborot xavfsizligini buzmaydigan tahdidlar**

B) Amalga oshishida axborot strukturasi va mazmunida hech narsani o'zgartirmaydigan tahdidlar

C) Texnik vositalar bilan bog'liq bo'lgan tahdidlar

D) Hech qachon amalga oshirilmaydigan tahdidlar

**161. Jumlani to'ldiring. Hujumchi kabi fikrlash ....  
Kerak.**

**A) Ma'lumot, axborot va tizimdan foydalanish uchun**

B) Ma'lumotni aniq va ishonchli ekanligini bilish uchun

C) Kafolatlangan amallarni ta'minlash uchun

**162. Axborot xavfsizligida zaiflik bu?**

**A) Tizim yoki tshkilotga zarar yetkazishi mumkin bo'lgan  
istalmagan hodisa**

B) Noaniqlikning maqsadlarga ta'siri

C) Tashkilot uchun qadrlı bo'lgan ixtiyoriy narsa

D) Tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson

**163. Jumlanı to'ldiring. Axborot xavfsızligıga bo'ladigan ... tahdidlari maqsadli (atayin) tahdidlar deb ataladi.**

A) Foydalanuvchilar va xizmat ko'rsatuvchi hodimlarning hatolıklari

B) Tabiiy ofat va avariya

C) Texnik vositalarning buzilishi va ishlamasligi

D) Strukturalarnı ruxsatsiz modifikatsiyalash

**164. .... – ushbu zaxiralash usuli tizim ishlamay turganda yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi. Ushbu usul zaxiralashning xavfsız usuli hisoblanib, ma'lumotni nusxalash xavfidan himoyalaydi.**

A) Issiq zaxiralash

B) Sovuq zaxiralash

- C) Iliq zaxiralash
- D) Ichki zaxiralash

**165. OSI modelining quyi sathi bu?**

**A) Fizik sath**

- B) Transport sathi
- C) Kanal sathi
- D) Tarmoq sathi

**166. Bir biriga osonlik bilan ma'lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi bu?**

**A) Tarmoq topologiyasi**

- B) Kompyuter topologiyasi
- C) Tarmoq arxitekturas
- D) Kompyuter tarmog'i

**167. Hajmi bo'yicha eng kichik hisoblangan tarmoq turi bu –**

**A) CAN**

B) PAN

C) MAN

D) LAN

**168. Tizimning turli resurslarga foydalanishni cheklash uchun foydalaniluvchi qoidalar to'plami haqidagi barcha narsalar bu?**

A) Avtorizatsiya

B) Autentifikatsiya

C) Identifikatsiya

D) Ruxsatlarni nazoratlash

**169. Bir xil baroshlika ega bo'lganida quyidagi algoritmlardan qaysi birida kalit uzunligi eng kata bo'ladi?**

A) DES

B) AES

C) A5/1

D) RSA

**170. 12 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating.**

**A) 14, 26**

B) 144, 4

C) 12 dan tashqari barcha sonlar

**D) 11, 13**

**171. Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?**

**A) Barcha javoblar to'g'ri**

B) Boshqa kompyuterda yozib olingan ma'lumotlarni o'qishdan oldin har bir saqlagichni antivirus tekshiruvidan o'tkazish

C) Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta'minlash va uni doimiy yangilab boorish

D) Faqat litsenziyali dasturiy ta'minotdan foydalanish

**172. Kirish hujumlari bu?**

**A) Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi**



- B) Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi
- C) Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi
- D) Tarmoq haqida axborotni to'plash hujumchilarga mavjud

**173. A5/1 algoritmidagi Z registor uzunligi nechiga teng?**

**A) 23**

- B) 21
- C) 22
- D) 19

**174. Ochiq tarmoq yordamida himoyalangan tarmoqni qurish imkoniyatiga ega himoya vositasi bu?**

**A) Antivirus**

- B) Tarmoqlararo ekran
- C) Virtual Private Network
- D) Router

**175. Diskni shifrlash usuliga xos bo'lgan xususiyatlarni belgilang.**

**A) Faqat kriptografik kalitlar xotirada saqlanib, shifrlangan fayllar ochiq holatda saqlanadi**

B) Asosiy fayl tizimining ustida joylashgan kriptografik fayl tizimidan foydalanish (masalan, ZSF, EncFS)

C) Deyarli barcha narsa, almashtirish maydoni (swap space), vaqtinchalik fayllar shifrlanadi

**176. Jumlani to'ldiring. Autentifikatsiya tizimlari asoslanishiga ko'ra .... turga bo'linadi.**

**A) 3**

B) 5

C) 4

D) 2

**177. Ikki kalitli kriptotizim bu –**

**A) MAC tizimlari**

B) Simmetrik kriptotizim

C) Ochiq kalitli kriptotizim

D) Xesh funksiyalar

**178. Kriptologiya so'ziga berilgan to'g'ri tavsifni toping?**

**A) Maxfiy shifrlarni buzish fani va san'ati**

B) Maxfiy shifrlarni yaratish fani va san'ati

C) Maxfiy shifrlarni yaratish, buzish fani va san'ati

D) Axborotni himoyalash fani va san'ati

**179. .... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to'plami.**

**A) Alifbo**

B) Kodlash

C) Shifrmavn

D) Ochiq matn

**180. Parollar 10 xonali uzunlikka va har bir xonasi uchun 14ta turli belgilar bo'lishi mumkin bo'lgan jami parollar soni nechta?**

**A)  $10^{14}$**

- B)  $14^{10}$
- C) 140
- D) 24

**181. Modul arifmetikasida mod9 bo'yicha 7 soniga teskari bo'lgan sonni toping?**

**A) 7/9**

- B) 4
- C) 63
- D) 2

**182. Paket filteri turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi?**

**A) Ilova sathi parametrlari asosida**

- B) Taqdimot sathi parametrlari asosida
- C) Tarmoq sathi parametrlari asosida
- D) Kanal sathi parametrlari asosida

**183. Kriptotizimning to'liq xavfsiz bo'lishi Kerxgovs prinsipiga ko'ra qaysi kattalikning nomalum bo'lishiga asoslanadi?**

**A) Algoritm**

B) Kalit

C) Protokol

D) Shifrmatn

**184. RSA algoritmidagi  $p=3$ ,  $q=11$  bo'lsa,  $N$  sonidan kichik va u bilan o'zaro tub bo'lgan sonlar miqdorini ko'rsating.**

**A) 43**

B) 20

C) 11

D) 13

**185. A5/1 algoritmidagi X registri uzunligi nechiga teng?**

**A) 23**

B) 19

C) 18

D) 22

**186. Qaysi himoya vositasi tomonlarni autentifikatsiyalash imkoniyatini beradi?**

A) Virtual private network

B) Tarmoqlararo ekran

C) Router

D) Antivirus

**187. Qaysi funksiya matnli fayllar bilan ishlashda mavjud put (joylashish) pozitsiyasini ifodalaydigan streampos turdagi qiymatni qaytaradi?**

A) Seekg()

B) Seekp()

C) Tellg()

D) Tellp()

**188. Foydalanuvchi yoki subyektni haqiqiyligini tekshirish jarayoni bu?**

**A) Autentifikatsiya**

B) Ruxsatlarni nazoratlash

C) Avtorizatsiya

D) Identifikatsiya

**189. Foydalanuvchi parollari bazada qanday ko'rinishda saqlanadi?**

**A) Bazada saqlanmaydi**

B) Xeshlangan ko'rinishda

C) Shifrlangan ko'rinishda

D) Ochiq holatda

**190. Qaysi bilim sohasi tashkil etuvchilar o'rtasidagi aloqani himoyalashga e'tibor qaratib, o'zida fizik va mantiqiy ulanishni birlashtiradi?**

**A) Dasturiy ta'minotlar xavfsizligi**

B) Ma'lumotlar xavfsizligi

- C) Aloqa xavfsizligi
- D) Tashkil etuvchilar xavfsizligi

**191. Ruxsatsiz foydalanish, qo'pol kuch hujumi, imtiyozni orttirish, o'rtaga turgan odam hujumi, kabilar qaysi tarmoq xavfsizligiga kiritilgan hujumlar oilasiga tegishli?**

**A) Razvedka hujumlari**

- B) Zararli hujumlar
- C) Xizmatdan voz kechishga undash hujumlari
- D) Kirish hujumlari

**192. Axborot xavfsizligida tahdid bu?**

**A) Noaniqlikning maqsadlarga ta'siri**

- B) Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa
- C) Aktivga zarar yetkazishi mumkin bo'lgan istalmagan hodisa
- D) U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz

**193. Xavfsizlik bo'shlig'i bo'lib, turli foydalanuvchilarni autentifikatsiyalash usullarini**



**aylanib o'tib hujumchiga tizimga kirish  
imkoniyatini taqdim etadi. Gap nima haqida  
bormoqda?**

**A) Zaiflik**

B) Aktiv

C) Tahdid

D) Hujum

**194. Yaxlitlikni ta'minlash bu-?**

**A) Ruxsatsiz bajarishdan himoyalash**

B) Ruxsatsiz yozishdan himoyalash

C) Ruxsatsiz o'qishdan himoyalash

D) Ruxsat etilgan amallarni bajarish

**195. Plastik kartadan to'lovni amalga oshirishda  
mavjud autentifikatsiya usuli qaysi sinfga tegishli?**

**A) Bir faktorli autentifikatsiya**

B) Ikki faktorli autentifikatsiya

C) Tokenga asoslangan autentifikatsiya

D) Biometrik autentifikatsiya

**196. RAID 0 texnologiyasining vazifasi –**

**A) Diskni navbatlanishi va xatolikni nazoratlash**

B) Diskni navbatlanishi

C) Bloklarni navbatlash va akslantirish

D) Diskni akslantirish

**197. Razvedka hujumlari bu?**

**A) Tizimni fizik buzishni maqsad qiladi**

B) Foydalanuvchilarga va tashkilotlarga mavjud bo'lgan biror xizmatni cheklashga urinadi

C) Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi

D) Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi

**198. Qaysi xususiyatlar RAID texnologiyasiga xos emas?**

**A) Disklarni “qaynoq almashtirish” mumkin**

B) Xatoliklarni nazoratlash mumkin

- C) Shaxsiy kompyuterda foydalanish mumkin
- D) Serverlarda foydalanish mumkin

**199. Axborotni mavjudligini yashirish bilan shug'ullanuvchi fan sohasi bu –**

**A) Kodlash**

- B) Steganografiya
- C) Kriptotahlil
- D) Kriptografiya

**200. Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lish. Gap qaysi ijtimoiy injineriya yo'nalishi haqida ketmoqda?**

**A) Barcha javoblar to'g'ri**

- B) Phishing
- C) Protexting
- D) Spoofing

**201.  $C = P \text{ XOR } K$  – bir martali bloknotda shifrlash funksiyasi bo'lsa, unga mos deshifrlash funksiyasini ko'rsating? Bu yerda, P- ochiq kalit, K-kalit, C-shifrmata**

**A)  $P = C \text{ AND } K$**

B)  $P = C \text{ OR } K$

C)  $P = C \text{ XOR } K$

D)  $P = C - K$

**202. Biror narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilari tushuniladi?**

**A) Token, mashinaning kaliti**

B) Yuz tasviri, barmoq izi

C) Biometrik parametrlar

D) PIN, Parol

**203. Qaysi biometrik parameter eng yuqori universallik xususiyatiga ega?**

**A) Yuz tasviri**

- B) Barmoq izi
- C) Qo'l shakli
- D) Ko'z qorachig'i

**204. Foydalanuvchi shaxsiy xabarlarini alohida shifrlashni unutgan vaqtlarda juda qo'l keladi. Gap qaysi shifrlash usuli xususida bormoqda?**

**A) Apparat shifrlash**

- B) Faylni shifrlash
- C) Dasturiy shifrlash
- D) Diskni shifrlash

**205. Faktorlash muammosi asosida yaratilgan assimetrik shifrlash usuli.**

**A) El-Gamal**

- B) Elliptik egri chiziqqa asoslangan shifrlash
- C) RSA
- D) Diffi-Xelman

**206. 64 ta belgidan iborat Sezar shifrlash usulida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin?**

**A) 32**

B) 63!

C)  $32^2$

D) 63

**207. “Yelka orqali qarash” hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan?**

**A) Biometrik autentifikatsiya**

B) Tokenga asoslangan autentifikatsiya

C) Ko'z qorachig'iga asoslangan autentifikatsiya

D) Parolga asoslangan autentifikatsiya

**208. Odatda mavjud bo'lgan IP – paket to'liq shifrlanib, unga yangi IP sarlavha beriladi. Ushbu amal qaysi himoya vositasida amalga oshiriladi?**

**A) Antivirus vositasi**

- B) Virtual xususiy tarmoq
- C) Diskni shifrlash vositasi
- D) Tarmoqlararo ekran

**209. Quyidagi ta'rif windows OTdagi qaysi hodisani tavsiflaydi? Ma'lumotni yo'qotish yoki funktsionallikni yo'qotish kabi muhim muammoni ko'rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, ..... hodisasi qayd etiladi.**

**A) Axborot**

- B) Muvaffaqiyatli audit
- C) Xatolik
- D) Ogohlantirish

**210. Elektron ma'lumotlarni yo'q qilishda maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o'zgaririladigan usul bu ....**

**A) Magnitsizlantirish**

- B) Shredirlash
- C) Yanchish
- D) Formatlash

**211. Virus aniq bo'lganda va xususiyatlari aniq ajratilgan holatda eng katta samaradorlikka ega zararli dasturni aniqlash usulini ko'rsating?**

**A) Anomaliyaga asoslangan usul**

- B) Signaturaga asoslangan usul
- C) Barcha javoblar to'g'ri
- D) O'zgarishga asoslangan usul

**212. O'zini yaxshi va foydali dasturiy vosita sifatida ko'rsatuvchi zararli dastur turi bu?**

**A) Backdoors**

- B) Trojan otlari
- C) Adware
- D) Spyware



**213. Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ..... amalga oshiriladi.**

**A) Yashirish**

B) Kodlash

C) Deshifrlash

D) Shifrlash

**214. Jumlani to'ldiring. Tizimli fikrlash .... uchun kerak.**

**A) Ma'lumot, axborot va tizimdan foydalanish**

B) Kafolatlangan amallarni ta'minlash

C) Ma'lumotni aniq va ishonchli ekanligini bilish

D) Bo'lishi mumkin bo'lgan xavfni oldini olish

**215. Ma'lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi?**

**A) Zarur axborotni tanlashdan**

B) Mos RAID sathini tanlashdan

C) Mos zaxira nusxalash vositasini tanlashdan

D) Mos zaxira nusxalash usulini tanlashdan

**216. Operatsion tizimlarda keng qo'llaniluvchi foydalanishni boshqarish usuli bu?**

**A) DAC**

B) MAC

C) RBAC

D) ABAC

**217. TCP/IP modelidagi ilova sathi OSI modelidagi qaysi sathlarga mos keladi?**

**A) Ilova, taqdimot va seans**

B) Ilova

C) Ilova va taqdimot

D) Seans va taqdimot

**218. Yaratilishi uchun faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmi nomini ko'rsating?**

**A) DES**

- B) El-Gamal
- C) A5/1
- D) RSA

**219. Shaxsiy simsiz tarmoqlar qo'llanilish sohasini belgilang.**

**A) Tashqi qurilmalar kabellaring o'rnida**

- B) Binolar va korxonalar va internet orasida belgilangan simsiz bog'lanish
- C) Butun dunyo bo'yicha internetdan foydalanishda
- D) Simli tarmoqlarni mobil kengaytirish

**220. Agar ob'ektning xavfsizlik darajasi sub'ektning xavfsizlik darajasidan kichik yoki teng bo'lsa, u holda o'qish uchun ruxsat beriladi. Ushbu qoida qaysi foydalanishni boshqarish usuliga tegishli.**

**A) ABAC**

- B) MAC
- C) RMAC

D) DAC

**221. Qaysi bilim sohasi foydalanilayotgan tizim yoki axborot xavfsizligini ta'minlovchi dasturiy ta'minotlarni ishlab chiqish va foydalanish jarayoniga e'tibor qaratadi?**

**A) Tashkil etuvchilar xavfsizligi**

B) Ma'lumotlar xavfsizligi

C) Dasturiy ta'minotlar xavfsizligi

D) Aloqa xavfsizligi

**222. RSA algoritmda  $p=5$   $q=13$   $e=7$  ga teng bo'lsa, shaxsiy kalitni hisoblang?**

**A) 7**

B) 65

C) 35

D) 13

**223. DNS serverlari tarmoqda qanday vazifani amalga oshiradi?**

**A) Tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq uchun chiqish nuqtasi vazifasini bajaradi**

B) Internet orqali ma'lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlash funksiyasini amalga oshiradi

C) Ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq uchun kiruvchi nuqta vazifasini bajaradi

**D) Xost nomlari va internet nomlarini IP manzillarga o'zgartirish va teskarisini amalga oshiradi**

**224. VPNning texnik amalga oshirilishiga ko'ra turlari keltirilgan qatorni toping.**

**E) Kanal sathidagi VPN; tarmoq sathidagi VPN; seans sathidagi VPN**

F) Dasturiy ko'rinishdagi VPN; maxsus shifrlash protsessoriga ega apparat vosita ko'rinishidagi VPN

G) Marshuritizator ko'rinishidagi VPN; tarmoqlararo ko'rinishidagi VPN

E) Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN

**225. Quyidagilardan qaysilari tarmoq topologiyalari hisoblanadi?**

**A) Halqa, yulduz, shina, daraxt**

B) UDP, TCP/IP, FTP

C) SMTP, HTTP, UDP

D) OSI, TCP/IP

**226. Jumlani to'ldiring. Parol kalitdan ..... farq qiladi.**

**A) Uzunligi bilan**

B) Tasodifiylik darajasi bilan

C) Belgilari bilan

D) Samaradorligi bilan

**227. Portlarni va operatsion tizimni skanerlash razvedka hujumlarining qaysi turida amalga oshiriladi?**

**A) Passiv**

B) Lug'atga asoslangan

C) DNS izi

D) Aktiv

Tuzuvchi: [@ocoderx](#)

Tahrirlovchi: [@its\\_mavjuda](#)