

Kanalimiz : TATU1K [https://t.me/+Nmbnri\\_d8Y4MTZi](https://t.me/+Nmbnri_d8Y4MTZi)

Gruhimiz : YORDAM <https://t.me/+0za4PE4Uk7c5MDU6>

Biz bilan bo'ling va 0 kiridit yig'ing ☺

1. Elektron axborot saqlovchilardan qayta foydalanishli ma'lumotlarni yo'q qilish usullari orasidan eng ishonchlisini aniqlang.
  - A) Formatlash
  - B) Delete buyrug'i yordamida o'chirish
  - C) Shift+Delete buyrug'i 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 himoyalangan 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) FOCT

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) Kriptogtafik himoya
  - C) Ma'lumotlarni zaxira nusxalash**
  - D) Tarmoqlararo ekran
24. Sub'ekt.lavozimi=Vrach & muhit.vaqtl >= 8:00 & muhit.vaqtl <= 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) Diskretsiyon 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'rish" 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.

- E) 10
- F) 13**
- G) 40
- H) 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) Muvaqqiyatli 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) Protexing

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'lmaslik
- 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) Protexting
- 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 algoritmda 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 registor 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 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 $\varphi(N)$  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 himoyalanganmagan ochiq tarmoq segmentli sxema; bo'lingan himoyalangan yopiq va ochiq segmentli tarmoq sxemasi

73. Ochiq matn qismlarini takroriy shifrlovchi 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 arxitekturas

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 algoritmidagi 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 parametrlarni almashtirish hujumi, zararli 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 algoritmidagi  $p=7$ ,  $q=11$ ,  $e=7$  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 mavjudligi

**B) *Nazoratlanmaydigan hududni har doim mavjudligi***

C) Xizmat ko'rsatishdan voz kechish hujumini mavjudligi

D) O'rtaga 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 vositasining 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 algoritmidagi maj(1,0,1) ga bo'lsa, qaysi registorlar siljiydi?

- A) X,Y,Z
- B) Y
- C) X,Z**

D) X,Y

110. RSA algoritmda  $p=7$ ,  $q=19$  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 algoritmda 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 algoritmda 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) Trojan 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 algoritmidagi 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 algoritmidagi registrlar siljiganidan keyingi 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 funktsiya 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 algoritmidagi  $p=5$   $q=11$   $e=7$  ga teng bo'lsa, shaxsiy kalitni hisoblang.

- A) **23**
- B) 35
- C) 24
- D) 7

133. Himoya mexanizmini aylanib o'tib tizimga ruxsatsiz kirish imkonini beruvchi zararli 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?

- A) Ikki ta 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 funktsionallikni 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 tashkilotga 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. Jumlani to'ldiring. Axborot xavfsizligiga bo'ladigan ... tahdidlari maqsadli (atayin) tahdidlar deb ataladi.

**A) Foydalanuvchilar va xizmat ko'rsatuvchi hodimlarning hatoliklari**

B) Tabiiy ofat va avariya

C) Texnik vositalarning buzilishi va ishlamasligi

D) Strukturalarni ruxsatsiz modifikatsiyalash

164. .... – ushbu zaxiralash usuli tizim ishlamay turganda yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi. Ushbu usul zaxiralashning xavfsiz 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 registori 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 Kerxgova prinsipiga ko'ra qaysi kattalikning nomalum bo'lishiga asoslanadi?

- A) Algoritm
- B) Kalit**
- C) Protokol
- D) Shifratn

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 funktsiya matnli fayllar bilan ishlashda mavjud put (joylashish) pozitsiyasini ifodalaydigan streampos turdagi qiymatni qaytaradi?

- A) Seekg()
- B) Seekp()
- C) Tellg()
- D) Tellp()**

188. Foydalanuvchi yoki subyektning haqiqiylikni 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 qadrlil 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-shifmatn

- 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 xabarlarni 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 funkcionallikni 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 samaradorlika 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 algoritmidagi  $p=5$   $q=13$   $e=7$  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**

