1. Elektron axborot saqlovchilardan qayta foydalanishli ma’lumotlarni yo’q qilish usullari orasidan eng ishonchlisini aniqlang.
   1. Formatlash
   2. Delete buyrug’I yordamida o’chirish
   3. Shift+Delete buyrug’I yordamida o’chirish

## Takroriy qayta yozish

1. 5 XOR 8 =? Natijani hisoblang.

## 13

* 1. 10
  2. 11
  3. 40

1. Agar a – ochiq kalit, b – shaxsi kalit, H – xabar, X() – xesh funksiya bo’lsa Sign() – imzolash funksiyasi uchun asosiy parametrlariga asoslangan ko’rinishini ko’rsating.
   1. Sign(X(H), a)
   2. Sign(H, a)
   3. Sign(H, b)

## Sign(X(H), b)

1. Ma’lumotni to’liq qayta tiklash qachon samarali amalga oshiriladi?
   1. Formatlash asosida ma’lumot o’chirilgan bo’lsa

## Saqlagichda ma’lumot qayta yozilmagan bo’lsa

* 1. Ma’lumotni o’chirish Delete buyrug’I bilan amalga oshirilgan bo’lsa
  2. Ma’lumotni o’chirish Shift+Delete buyrug’I bilan amalga oshirilgan bo’lsa

1. …… - ushbu zaxiralashda tarmoqqa bog’lanish amalga oshiriladi. Ushbu zaxiralashda, tizim yangilanishi davomiy yangilanishni qabul qilish uchun ulanadi.
   1. Issiq zaxiralash
   2. Ichki zaxiralash

## Iliq zaxiralash

* 1. Sovuq zaxiralash

1. 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?
   1. Hisoblash uchun shartlar yetarli emas

## 128

* 1. 64
  2. 256

1. Sotsial injeneriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan?
   1. Biometrik autentifikatsiya
   2. Ko’z qorachig’iga asoslangan autentifikatsiya
   3. Tokenga asoslagan autentifikatsiya

## Parolga asoslangan autentifikatsiya

1. 2 XOR 6 = ? Natijani hisoblang.

## 4

* 1. 6
  2. 8
  3. 12

1. VPNning texnik yechim arxitekturasiga ko’ra turlari keltirilgan qatorni toping.
   1. Kanal sathidagi VPN; tarmoq sathidagi VPN; seans sathidagi VPN
   2. Dasturiy ko’rinishdagi VPN; maxsus shifrlash protsessoriga ega apparat vosita ko’rinishidagi VPN
   3. Marshuritizator ko’rinishidagi VPN; tarmoqlararo ko’rinishidagi VPN

## Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN

1. 6 XOR 6 = ? Natijani hisoblang.

## 0

* 1. 6
  2. 12
  3. 36

1. Parolga xos bo’lmagan xususiyatni ko’rsating.
   1. Klaviatura orqali barcha kiritiluvchi qiymatlarni qabul qiladi
   2. PIN kodni parolni xususiy holati sifatida qarash mumkin
   3. Ixtiyoriy uzunlikda bo’lishi mumkin

## Faqat pechat qilinuvchi belgilarni qabul qiladi

1. Tarmoqlararo ekran vositasi bajarilishiga ko’ra qanday turlarga bo’linadi?
   1. Paket filterlari – tarmoq sathida ishlaydi, ekspert paketi filterlari – transport sathida ishlaydi; ilova proksilari – ilova sathida ishlaydi
   2. Yagona tarmoq himoyasi sxemasi; himoyalangan yopiq va himoyalanmagan ochiq tarmoq segmentli sxema; bo’lingan himoyalangan yopiq va ochiq segmentli tarmoq sxemasi

## Apparat-dasturiy: Dasturiy

* 1. Protokol holatini nazoratlash: vositachi yordamida(proksi)

1. GSM tarmog’ida ovozli so’zlashuvlarni shifrlash algoritmi bu?
   1. RSA

# A5/1

* 1. ГОСТ
  2. DES

1. Xavfsizlik siyosati xususiyatlari keltirilgan qatorni ko’rsating.
   1. Tushunarli bo’lishi, amaliy bo’lishi

## Barcha javoblar to’g’ri

* 1. Qisqa va aniq foydalanuvchan bo’lishi
  2. Iqtisodiy asoslangan bo’lishi

1. 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).

# I(02)

* 1. Berilgan shartlar yetarli emas
  2. I(01) va I(02) ga bog’liq emas
  3. I(01)

1. Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi?
   1. Antivirus
   2. Router

## Tarmoqlararo ekran

* 1. Virtual himoyalangan tarmoq

1. Elektron raqamli imzo keltirilganlardan qaysi xususiyatni ta’minlamaydi?
   1. Yaxlitlik
   2. Qalbakilashtirishdan himoya

## Konfidensiallik

* 1. Rad etishdan himoya

1. 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?
   1. Quyi
   2. Barcha
   3. Yuqori

## O’rta

1. Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo’shimcha apparat va dasturiy vositani talab qiladi?
   1. USB disklar
   2. Ko’chma qattiq disklar
   3. CD/DVD disklar

## Lentali disklar

1. Eng zaif simsiz tarmoq protokolini ko’rsating.
   1. WPA3

# WEP

* 1. WPA2
  2. WPA

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

## Tahdidchi ishini oshirish

* 1. Murakkab parol hosil qilish
  2. Yana bir maxfiy parametr kiritish
  3. Murakkab xesh qiymat qiymat hosil qilish

1. *(Bob-), (Alisa,rw), (Sem,rw), (buxgalteriyaga oid dastur,rw).* Ushbu qoida quyidagilardan qaysi biriga tegishli?
   1. Biba modeli
   2. Imtiyozlar ro’yhati yoki C-list

## Foydalanishni boshqarish ro’yhati yoki ACL

* 1. Foydalanishni boshqarish matritsasi

1. Jumlani to’ldiring. …… - muhim bo’lgan avborot nusxalash yoki saqlash jarayoni bo’lib, bu ma’lumot yo’qolgan vaqtda qayta tiklash imkoniyatini beradi.
   1. VPN
   2. Kriptogtafik himoya

## Ma’lumotlarni zaxira nusxalash

* 1. Tarmoqlararo ekran

1. Sub’ekt.lavozimi=Vrach & muhit.vaqt >= 8:00 & muhit.vaqt <= 18:00. Ushbu keltirilgan shart qaysi foydalanishni boshqarish usuliga tegishli?
   1. Rolga asoslangan foydalanishni boshqarish
   2. Mandatli foydalanishmi boshqarish

## Attributga asoslangan foydalanishni boshqarish

* 1. Diskretsion foydalanishni boshqarish

1. Trafik orqali axborotni to’plashga harakat qilish razvedka hujumlarining qaysi turida amalga oshiriladi?
   1. Lug’atga asoslangan

## Passiv

* 1. DNS izi
  2. Aktiv

1. Modul arifmetikasida mod7 bo’yicha 4 soniga teskari bo’lgan sonni toping?

A) ¼

# B) 2

C) 4

D) 7

1. A5/1 shifrlash algoritmida registrlar siljiganidan keying holat: x18=0, y21=1 va z22=1 ga teng bo’lsa, hosil bo’lgan psevdotasodifiy qiymatni ko’rsating.

## 0

* 1. 11
  2. 1
  3. 110

1. Zaxiralashni amalga oshirishda inson ishtirokini talab etadi; Tabiiy-ofatlarga yoki o’g’irlashga moyil. Ushbu xususiyat qaysi zaxira nusxalash manziliga tegishli?
   1. Bulutli tizmda zaxiralash
   2. Barcha javoblar to’g’ri
   3. Tashqi (offsite) zaxiralash

## Ichki (onsite) zaxiralash

1. Resurslardan foydalanish usuliga ko’ra kompyuter viruslari qanday turlarga bo’linadi?
   1. Shifrlangan, shifrlanmagan va polimorf
   2. Dasturiy, yuklanuvchi, makroviruslar va ko’p platformali
   3. Resident va norezident

## Virus-parazitlar va virus-chervlar

1. Risk ta’sirini kamaytirish uchun profilaktika choralarini ko’rish zarur. Mazkur harakatlar riskning qaysi darajasi uchin?
   1. Barcha

## Quyi

* 1. O’rta
  2. Yuqori

1. TCP/IP modelidagi kanal sathi OSI modelidagi qaysi sathlarga mos keladi?
   1. Tarmoq va kanal
   2. Kanal

## Fizik va kanal

* 1. Fizik

1. “Kompilyator foydalanuvchining imtiyoziga ko’ra ish ko’rish o’rniga o’zining imtiyoziga asosan ish ko’rishi” klassik xavfsizlik sohasida nima deb yuritiladi?
   1. Donadorlik muammosi
   2. Klassifikatsiyalashdagi muammo
   3. Cheklanishdagi muammo

## Tartibsiz yordamchi muammosi

1. 2 XOR 4 = ? Natijani hisoblang.

# A) 6

B) 4

C) 2

D) 8

1. 5 XOR 8 = ? Natijani hisoblang.
2. 10

## 13

1. 40
2. 12
3. Markaziy xab yoki tugun orqali tarmoqni markazlashgan holda boshqarish qaysi tarmoq topologiyasida amalga oshiriladi?
   1. Mesh
   2. Xalqa
   3. Shina

## Yulduz

1. Yaratishda psevdotasofiy sonlar generatoriga asoslanuvchi kriptografik shifrlash usuli bu?
   1. Ochiq kalitli
   2. Assimmetrik
   3. Simmetrik blokli

## Simmetrik oqimli

1. 4 XOR 4 = ? Natijani hisoblang.

## 0

* 1. 8
  2. 16
  3. 4

1. Elektron raqamli imzo muolajalarini ko’rsating.
   1. Imzoni shakllantirish va xeshlash
   2. Imzoni xeshlash va xesh matni deshifrlash
   3. Shifrlash va deshifrlash

## Imzoni shakllantirish va imzoni tekshirish

1. Foydalanuvchining tizimga muvaffaqiyatli urinishi Windows OT da qanday audit hodisasi sifatida qayd etiladi?
   1. Muvaffaqiyatsiz audit
   2. Ogohlantirish
   3. Xatolik

## Muvaffaqiyatli audit

1. Ushbu hujumda foydalanuvchilarning akkauntlari bloklangani va kredit karta ma’lumotlari blokdan chiqarilishi kerakli to’g’risidagi ma’lumot foydalanuvchi electron pochtalariga yuboriladi. Gap qaysi ijtimoiy injeneriya turi haqida bormoqda?

## Phishing

* 1. Spoofing
  2. Protexting
  3. Barcha javoblar to’g’ri

1. Ma’lumotni zaxira nusxalash nima uchun potensial tahdidlarni paydo bo’lish ehtimolini oshiradi?

## Tahdidchi uchun nishon ko’payadi

* 1. Ma’lumot yo’qolgan taqdirda ham tiklash imkoniyati mavjud bo’ladi
  2. Saqlanuvchi ma’lumot hajmi ortadi
  3. Ma’lumotni butunligi ta’minlanadi

1. Manbaga zarar keltiradigan ichki va tashqi zaiflik ta’sirida tahdid qilish ehtimoli bu?
   1. Hujum
   2. Zaiflik

## Risk

* 1. Tahdid

1. RSA algoritmida ochiq kalit e=5, N=35 ga teng bo’lsa, M=3 ga teng ochiq matnni shifrlash natijasini ko’rsating.
   1. 35
   2. 7
   3. 5

## 33

1. RAID 3 texnologiyasing vazifasi –

## Diskni navbatlanishi va xatolikni nazoratlash

* 1. Bloklarni navbatlash va akslantirish
  2. Diskni navbatlanishi
  3. Diskni akslantirish

1. RSA algoritmida p=3, q=11 bo’lsa, N sonidan kichik va u bilan o’zaro tub bo’lgan sonlar miqdorini ko’rsating.
   1. 14
   2. 33

## 20

* 1. 12

1. Resursni va harakatni kim bajarayotgani to’g’risidagi holatlar “AGAR, U HOLDA” dan tashkil topgan qoidalarga asoslanadi. Gap qaysi foydalanishni boshqarish usuli haqida bormoqda?
   1. DAC
   2. MAC
   3. RBAC

# ABAC

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

## Risk

* 1. Hujum
  2. Tahdid
  3. Zaiflik

1. Jumlani to’ldiring. Tarmoqlararo ekranning vazifasi …
   1. Tarmoq hujumlarini aniqlash
   2. Tarmoqdagi xabarlar oqimini uzish va ulash

## Ishonchli va ishonchsiz tarmoqlar orasida ma’lumotlarga kirishni boshqarish

* 1. Trafikni taqiqlash

1. Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan?
   1. Apparat nazoratlash

## Ma’muriy nazoratlash

* 1. Texnik nazoratlash
  2. Fizik nazoratlash

1. RSA algoritmida p=7, q=5 bo’lsa, N sonidan kichik va u bilan o’zaro tub bo’lgan sonlar miqdorini ko’rsating.

## 24

* 1. 35
  2. 12
  3. 60

1. Foydalanishni boshqarish matritsasi ustunlar bo’yicha bo’linsa … hosil bo’ladi.

## Foydalanishni boshqarish ro’yhati yoki ACL

* 1. Foydalanishni boshqarish matritsasi
  2. Imtiyozlar ro’yhati yoki C-list
  3. Biba modeli

1. 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?

* 1. Anomaliyaga asoslangan
  2. Signaturaga asoslangan

## O’zgarishni aniqlashga asoslangan

* 1. Barchasiga

1. Parollarni saqlashda nega shifrlashning o’rniga xeshlash amalidan foydalaniladi?
   1. Shifrlash algoritmlari xavfsiz emas
   2. Shifrlash algoritmlari tezkor emas
   3. Xesh funksiyalari xavfsiz

## Shifrlash kalitini saqlash zaruriyati mavjud

1. Modul arifmetikasida mod7 bo’yicha 5 soniga teskari bo’lgan sonni toping?

## 3

* 1. 35
  2. 2
  3. 5/7

1. Voqea sodir bo’lish ehtimoli va ushbu hodisaning axborot texnologiyalari aktivlariga ta’siri bu?
   1. Hujum
   2. Tahdid
   3. Zaiflik

## Risk

1. Kriptografiya so’ziga berilgan to’g’ri tavsifni toping?
   1. Maxfiy shifrlarni yaratish va buzish fani va san’ati

## Maxfiy shifrlarni yaratish fani va san’ati

* 1. Axborotni himoyalash fani va san’ati
  2. Maxfiy shifrlarni buzish fani va san’ati

1. Asosiy maqsad ma’lumotni maxfiyligini ta’minlash bo’lgan jarayonni ko’rsating?
   1. Dekodlash
   2. Kodlash

## Shifrlash

* 1. Deshifrlash

1. Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting.
   1. Almashib bo’lmaslik
   2. Doimo esda saqlash zaruriyati

## Doimo xavfsiz saqlab olib yurish zaruriyati

* 1. Qalbakilashtirish muammosi mavjudligi

1. 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.
   1. Sign(X, d)
   2. Sign(X, e)
   3. Sign(H(X), d)

## Sign(H(X), e)

1. RSA algoritmida p=5, q=11 bo’lsa, N sonidan kichik va u bilan o’zaro tub bo’lgan sonlar miqdorini ko’rsating.
   1. 55
   2. 10
   3. 11

## 40

1. Paydo bo’lishi tasodifiy, qasddan yoki boshqa harakatning ta’sirida bo’lishi mumkin bo’lgan hodisa bu?

## Tahdid

* 1. Aktiv
  2. Hujum
  3. Zaiflik

1. 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?

* 1. O’rta

## Yuqori

* 1. Quyi
  2. Barcha

1. 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?

* 1. Barcha javoblar to’g’ri
  2. Protexting

## Phishing

* 1. Spoofing

1. 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?
   1. Kibernetika
   2. Kiberxavfsizlik

## Ijtimoiy injeneriya

* 1. Kiberjinoyatlar

1. A5/1 oqimli shifrlash algoritmida maj(1,1,1) ga bo’lsa, qaysi registorlar siljiydi?
   1. Y

# X,Y,Z

* 1. X,Y
  2. X,Z

1. Ochiq kalitli kriptotizimda ma’lumotga imzo qo’yish qaysi kalit yordamida amalga oshiriladi?
   1. Yuboruvchining ochiq kaliti
   2. Qabul qiluvchining ochiq kaliti

## Yuboruvchining shaxsiy kaliti

* 1. Qabul qiluvchining shaxsiy kaliti

1. Modul arifmetikasida mod11 bo’yicha 3 soniga teskari bo’lgan sonni toping?
   1. 5
   2. 1/11

## 4

* 1. 1/3

1. A5/1 algoritmidagi Y registor uzunligi nechiga teng?
   1. 21

## 22

* 1. 23
  2. 19

1. RSA algoritmidagi ochiq va shaxsiy kalitlar uchun qanday munosabat o’rinli?
   1. Ochiq va shaxsiy kalitlar mod(p\*q) bo’yicha o’zaro teskari
   2. Ochiq va shaxsiy kalitlar uchun biror munosabat o’rinli emas
   3. Ochiq va shaxsiy kalitlar modN bo’yicha o’zaro teskari

## Ochiq va shaxsiy kalitlar modϕ(N) bo’yicha o’zaro teskari

1. Eng kam vaqtda ma’lumotni tiklash imkoniyatiga ega usul bu?

## Differensial zaxiralash

* 1. O’sib boruvchi zaxiralash
  2. To’liq zaxiralash
  3. Ichki zaxiralash

1. Qurbon kompyuteridagi ma’lumotni shifrlab, uni deshifrlash uchun to’lovni amalga oshirishni talab qiluvchi zararli dastur bu-?
   1. Rootkits
   2. Mantiqiy bombalar
   3. Spyware

## Ransomware

1. Tarmoqlararo ekran vositasi OSI modeling funksional sathlari bo’yicha qanday turlarga bo’linadi?

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

* 1. Protokl holatini nazoratlash; vositachi yordamida nazoratlash (proksi)
  2. Apparat-dasturiy; dasturiy
  3. Yagona tarmoq himoyasi sxemasi; himoyalangan yopiq va himoyalanmagan ochiq tarmoq segmentli sxema; bo’lingan himoyalangan yopiq va ochiq segmentli tarmoq sxemasi

1. Ochiq matn qismlarini takroriy shifrlovchi algoritmlar bu –

## Blokli shifrlar

* 1. Ochiq kalitli shifrlar
  2. Asimmetrik shifrlar
  3. Oqimli shifrlash

1. Ma’lumot shifrlansa, natijasi …. bo’ladi.
   1. No’malum
   2. Ochiq matn
   3. Kod

## Shifrmatn

1. Tarmoqdagi barcha tugunlarni o’zaro bog’laydi. Gap qaysi topologiya haqida bormoqda?

## Halqa

* 1. Yulduz
  2. Shina
  3. Daraxt

1. Agar simmetrik oqimli shifrlash algoritmida kiritilgan ochiq matn uzunligi 256 bitga teng bo’lsa, shifrmatn uzunligi necha bit bo’ladi?
   1. 128

## 256

* 1. 4
  2. 64

1. Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu?
   1. Identifikatsiya
   2. Autentifikatsiya
   3. Ro’yxatga olish

## Avtorizatsiya

1. Parollar 10 xonali uzunlikka va har bir xonasi uchun 16ta turli belgilar bo’lishi mumkin bo’lgan jami parollar soni nechta?
   1. 26
   2. 160
   3. 10^16

## 16^10

1. Shaxsni kimdir deb davo qilish jarayoni bu?
   1. Ruxsatlarni nazoratlash
   2. Avtorizatsiya
   3. Autentifikatsiya

## Identifikatsiya

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

## Kanal sathidagi vpn; tarmoq sathidagi vpn; seans sathidagi vpn

* 1. Dasturiy ko’rinishdagi vpn; maxsus shifrlash protsessoriga ega apparat vosita ko’rinishidagi vpn
  2. Korporativ tarmoq ichidagi vpn; masofadan foydalaniluvchi vpn; korporativ tarmoqlararo vpn
  3. Marshuritizator ko’rinishidagi vpn; tarmoqlararo ekran ko’rinishidagi vpn

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

## Faylni shifrlash

* 1. Apparat shifrlash
  2. Diskni shifrlash

1. Yo’q qilish usullari orasidan ekologik jihatdan ma’qullanmaydigan va maxsus joy talab qiladigan usul qaysi?
   1. Ko’mish

## Yoqish

* 1. Kimyoviy ishlov berish
  2. Maydalash

1. Qaysi akslantirishda ochiq matndagi belgilarning takrorlanish chastotasi shifrmatndagi belgilarda ham bir xil bo’ladi?
   1. Bir alifboli o’rniga qo’yish
   2. Gammalash
   3. Qo’shish

## O’rin almashtirish

1. Blokli simmetrik shifrlashda shifrmatndagi bir bitning o’zgarishi deshifrlangan matndagi necha bitning o’zgarishiga olib keladi?
   1. Buni aniqlash imkonsiz

## 1

* 1. Barchasiga
  2. Kamida bir blokiga

1. [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?
   1. Protexting

## Phishing

* 1. Spoofing
  2. Barcha javoblar to’g’ri

1. Zaxira nusxalash manzillarini ko’rsating.
   1. To’liq, differensial va o’sib boruvchi zaxiralash
   2. Barcha javoblar to’g’ri
   3. Issiq, sovuq va iliq zaxiralash

## Ichki, tashqi va bulutda zaxiralash

1. AGAR talabgor boshqaruvchi bo’lsa, U HOLDA maxfiy ma’lumotni o’qish/yozish huquqi berilsin. Bu qaysi foydalanishni boshqarish usuliga misol bo’ladi?
   1. DAC
   2. RBAC
   3. MAC

# ABAC

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

A) 3

B) 1

C) 0

# D) 2

1. Bir-biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi bu?
   1. Tarmoq topologiyasi

## Kompyuter tarmog’i

* 1. Kompyuter topologiyasi
  2. Tarmoq arxitekturasi

1. Subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim etish jarayoni bu?
   1. Avtorizatsiya

## Identifikatsiya

* 1. Ruxsatlarni nazoratlash
  2. Autentifikatsiya

1. Foydalanishni boshqarishning qaysi usulida asosiy g’oya tizimning ishlash logikasini tashkilotdagi kadrlar vazifasiga yaqinlashtirishga harakat qilinadi?
   1. DAC

# RBAC

* 1. MAC
  2. ABAC

1. Yong’inga qarshi kurashishning aktiv usuli to’g’ri ko’rsatilgan javobni toping.
   1. Minimal darajada yonuvchan materiallardan foydalanish, qo’shimcha etaj va xonalar qurish
   2. Binoga istiqomat qiluvchilarni yong’in sodir bo’lganda qilinishi zarur bo’lgan ishlar bilan tanishtirish
   3. Yetarli sondagi qo’shimcha chiqish yo’llarini mavjudligi

## Tutunni aniqlovchilar, alangani aniqlovchilar va issiqlikni aniqlovchilar

1. A5/1 shifrlash algoritmida registrlar siljiganidan keying holat: x18=1, y21=1 va z22=1 ga teng bo’lsa, hosil bo’lgan psevdotasodifiy qiymatni ko’rsating.
   1. 0
   2. 11
   3. 111

## 1

1. Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko’rsating.
   1. Parollar lug’atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydalanish asisida hujum
   2. Parollar lug’atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararki dasturladan foydalanish asosida hujum

## Fizik o’g’irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar

* 1. Fizik o’g’irlash, yelka orqali qarash hujumi, zararli dasturlardan foydalanishga asoslangan hujumlar

1. Seans sathidagi VPN qaysi protocol asosida quriladi?
   1. IPsec
   2. PPTP
   3. L2F

# TLS

1. RSA algoritmida p=7, q=11, e=7 ga teng bo’lsa, shaxsiy kalitni hisoblang.

## 43

* 1. 7
  2. 77
  3. 11

1. Qaysi himoya vositasi mavjud IP – paketni to’liq shifrlab, unga yangi IP sarlavha beradi?
   1. Router
   2. Tarmoqlararo ekran

# VPN

* 1. Antivirus

1. Faqat simsiz tarmoqlarga xos bo’lgan zaifliklarni ko’rsating?
   1. Zararli dasturlardan foydalanishga asoslangan hujumlarni mavjudliligi

## Nazoratlanmaydigan hududni har doim mavjudligi

* 1. Xizmat ko’rsatishdan voz kechish hujumini mavjudligi
  2. O’rtaga turgan odam hujumini mavjudligi

1. Juda ahamiyatli emas, lekin kelajakda yuzaga kelishi mumkin bo’lgan

muammolarni ko’rsatishi mumkin bo’lgan voqealar Windows OTda qanday hodisa sifatida qayd etiladi?

* 1. Axborot
  2. Muvaffaqiyatsiz audit

## Ogohlantirish

* 1. Xatolik

1. 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?
   1. Barchasiga
   2. Signaturaga asoslangan
   3. O’zgarishni aniqlashga asoslangan

## Anomaliyaga asoslangan

1. Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo’lgan murojaatlarini chegaralash qaysi himoya vositasing vazifasi hisoblanadi?
   1. Antivirus
   2. Router

## Tarmoqlararo ekran

* 1. Virtual himoyalangan tarmoq

1. Tashqi ma’lumotlarni bazaga yuklashda qanday kengaytmali fayl formatidan foydalansa bo’ladi?
   1. JPEG
   2. PDF
   3. CSV
   4. DOCX
2. Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqiyatli o’rnatuvchi asos bu?

## Tarmoq modeli

* 1. Kompyuter tarmog’i
  2. Mobil tarmoq
  3. Tarmoq topologiyasi

1. WEP, WPA, WPA2 protokollari qaysi simsiz texnologiyada ishlatilgan?
   1. WiMax

## Wi-Fi

* 1. GSM
  2. Bluetooth

1. Zaxira nusxalash strategiyasi rejasi nimadan boshlanadi?
   1. Mos zaxira nusxalash usulini tanlashdan
   2. Zaxira nusxalash texnologiyasini tanlashdan
   3. Zaxira nusxalash uchun xotira qurilmasini tanlashdan

## Tashkilot missiyasi uchun zarur axborotni aniqlashdan

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

## Fizik xavfsizlik

* 1. Huquqiy xavfsizlik
  2. Tarmoq xavfsizligi

1. Xavfsizlik siyosatlarining afzalliklari keltirilgan qatorni toping.
   1. Kuchaytirilgan ma’lumot va tarmoq xavfsizligini ta’minlaydi
   2. Qurilmalardan foydalanish va ma’lumotlar transferining monitoringlanishi va nazoratlanishini ta’minlaydi

## Barcha javoblar to’g’ri

* 1. Risklarni kamaytiradi

1. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to’plami bu?
   1. Xavfsizlik doktorinasi

## Xavfsizlik siyosati

* 1. Xavfsizlik konsepsiyasi
  2. Tashkilot nizomi

1. A5/1 oqimli shifrlash algoritmida maj(1,0,1) ga bo’lsa, qaysi registorlar siljiydi?
   1. X,Y,Z
   2. Y

# X,Z

* 1. X,Y

1. RSA algoritmida p=7, q=19 bo’lsa, N sonidan kichik va u bilan o’zaro tub bo’lgan sonlar miqdorini ko’rsating.
   1. 133
   2. 26
   3. 72

## 108

1. A5/1 oqimli shifrlash algoritmida maj(0,1,0) ga bo’lsa, qaysi registorlar siljiydi?
   1. X,Y,Z

# Y

* 1. X,Z
  2. X,Y

1. Ochiq kalitli shifrlash algoritmida ma’lumotni shifrlab yuborish qaysi kalit yordamida amalga oshiriladi?
   1. Qabul qiluvchining shaxsiy kaliti
   2. Qabul qiluvchining ochiq kaliti

## Yuboruvchining shaxsiy kaliti

* 1. Yuboruvchining ochiq kaliti

1. Yong’inga qarshi tizimlarni aktiv chora turiga quyidagilardan qaysilari kiradi.
   1. Yong’inga aloqador tizimlarni to’g’ri madadlanganligi

## Yong’inni aniqlash va bartaraf etish tizimi

* 1. Minimal darajada yonuvchan materiallardan foydalanish
  2. Yetarlicha miqdorda qo’shimcha chiqish yo’llarini mavjudligi

1. Modul arifmetikasida mod11 bo’yicha 5 soniga teskari bo’lgan sonni toping?

## 9

* 1. 4
  2. 1/11
  3. 1/5

1. Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko’rish rejimini kuzatib boruvchi zararli dastur turi bu?
   1. Backdoors

## Adware

* 1. Spyware
  2. Troyan otlari

1. Kompyuter viruslarini tarqalish usullarini ko’rsating.
   1. Ma’lumot saqlovchilari, internetdan yuklab olish va skaner qurilmalari orqali
   2. Barcha javoblar to’g’ri

## Ma’lumot saqlovchilari, internetdan yuklab olish va electron pochta orqali

* 1. Printer qurilmasi, internetdan yuklab olish va electron pochta orqali

1. Riskning qaysi darajasida risk ta’sirini kamaytirish uchun profilaktika choralarini ko’rish talab etiladi?

## Quyi

* 1. Yuqori
  2. Barcha darajalarda
  3. O’rta

1. Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalaniladi?
   1. Apparat

## Dasturiy

* 1. Simmetrik
  2. Ochiq kalitli

1. RSA algoritmida ochiq kalit e=5 n=35 ga teng bo’lsa M=2 ga teng ochiq matnni shifrlash natijasini ko’rsating?
   1. 35
   2. 7
   3. 5

## 32

1. Modul arifmetikasida mod5 bo’yicha 4 soniga teskari bo’lgan sonni toping?
   1. 20
   2. 1

## 4

* 1. 4/5

1. A5/1 shifrlash algoritmida registrlar siljiganidan keying holat: x18=0, y21=0 va z22=1 ga teng bo’lsa, hosil bo’lgan psevdotasodifiy qiymatni

ko’rsating.

* 1. 100

## 0

* 1. 1
  2. 10

1. Simsiz lokal tarmoq texnologiyasini ko’rsating.
   1. Ethernet

## Wi-Fi

* 1. WiMax
  2. Bluetooth

1. Parollar 6 xonali uzunlikka va har bir xonasi uchun 32 ta turli belgilar bo’lishi mumkin bo’lgan jami parollar soni nechta?
   1. 6^32
   2. 32!

## 32^6

* 1. 6!

1. Har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo’shilsa ….
   1. Hujum paydo bo’ladi

## Risk paydo bo’ladi

* 1. Aktiv paydo bo’ladi
  2. Tahdid paydo bo’ladi

1. Faqat ma’lumotga nisbatan o’zgarish yuz berganda zaxiralashni amalga oshiruvchi usuli?
   1. Differensial zaxiralash
   2. To’liq zaxiralash

## O’sib boruvchi zaxiralash

* 1. Ichki zaxiralash

1. Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas.
   1. Turli kirishlar turli chiqishlarni akslantirishi
   2. Kolliziyaga bardoshli bo’lishi
   3. Amalga oshirishdagi yuqori tezkorlik

## Bir tomonlama funksiya bo’lmasligi kerak

1. Ob’yektning eng cheklangan imtiyoz turini aniqlang.
   1. Private
   2. Protected
   3. Static

## Public

1. Biror mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu?
   1. Virus
   2. Adware

## Mantiqiy bombalar

* 1. Backdoors

1. Quyidagi atamalardan qaysi biri faqat simmetrik blokli shifrlarga xos?

## Blok uzunligi

* 1. Kalit uzunligi
  2. Kodlash jadvali
  3. Ochiq kalit

1. Axborotni qaysi xususiyatlari ochiq kalitli shifrlar yordamida ta’minlanadi?
   1. Foydalanuvchanlik va konfidensiallik

## Konfidensiallik, butunlik va foydalanuvchanlik

* 1. Konfidensiallik
  2. Butunlik va foydalanuvchanlik

1. Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi?
   1. Antivirus
   2. Router

## Tarmoqlararo ekran

* 1. Virtual himoyalangan tarmoq

1. RSA algoritmida p=5 q=11 e=7 ga teng bo’lsa, shaxsiy kalitni hisoblang.

## 23

* 1. 35
  2. 24
  3. 7

1. Himoya mexanizmini aylanib o’tib tizimga ruxsatsi kirish imkonini beruvchi zarali dastur bu?
   1. Troyan otlari
   2. Adware
   3. Spyware

## Backdoors

1. Legitimate code

If hour is 7 p.m:

crash\_computer() legitimate code

Ushbu mantiqiy kod qaysi zararli dasturiy vositaga tegishli?

* 1. Adware

## Mantiqiy bomba

* 1. Virus
  2. Backdoors

1. Diskdagi barcha ma’lumotlarni ( master boot record, (MBR) bilan) yoki MBRsiz shifrlashni amalga oshiradi. Gap qaysi shifrlash usuli haqida bormoqda?
   1. Apparat shifrlash
   2. Dasturiy shifrlash
   3. Faylni shifrlash

## Diskni shifrlash

1. “Single-pair shortest path problem” ushbu atama nimani anglatadi?
   1. Ikkita tugun orasidagi eng qisqa masofani aniqlash masalasi
   2. Berilgan tugundan barcha tugunlarga bo’lgan qisqa yo’llarni aniqlash masalasi
   3. Berilgan punktga yetib borishning qisqaroq yo’lini aniqlash masalasi
   4. 3 ta tugun orasidagi eng qisqa masofani aniqlash masalasi
2. Tarmoqdagi kompyuterlarga kabel orqali ulangan markaziy xabdan (tugun) iborat topologiya nima?
   1. Shina
   2. Daraxt

## Yulduz

* 1. Halqa

1. Paketlarni snifferlash, portlarni skanerlash, ping buyru’gini yuborish qanday hujum turiga misol bo’ladi?
   1. Zararli hujumlar

## Razvedka hujumlari

* 1. Xizmatdan voz kechishga undash hujumlari
  2. Kirish hujumlari

1. Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi shifrlar bu –
   1. **Ochiq kalitli shifrlar**
   2. Xesh funksiyalar
   3. Bir xil kalitli shifrlar
   4. Simmetrik shifrlar
2. 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?
   1. MAC
   2. ABAC

# RBAC

* 1. DAC

1. Biba modelida axborotni qaysi xususiyatini ta’minlashni maqsad qiladi?
   1. Konfidensiallik

## Butunlik

* 1. Foydalanuvchanlik
  2. Maxfiylik

1. 2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo’yicha qo’shing?
   1. 11111
   2. 01100
   3. 10000

## 00001

1. Quyidagi muammolardan qaysi biri simmetrik kriptotizimlarga xos.
   1. Foydalanuvchilar tomonidan maqbul ko’rilmasligi
   2. Kalitlarni esda saqlash murakkabligi

## Kalitni taqsimlash zaruriyati

* 1. Shifrlash jarayonining ko’p vaqt olishi

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

## Xatolik

* 1. Ogohlantirish
  2. Muvaffaqiyatsiz audit
  3. Axborot

1. Mijozlar, foydalanuvchilar va tashkilotlarda mavjud bo’lgan biror xizmatni cheklashga urinuvchi hujum bu?
   1. Spufing hujumi
   2. Razvedka hujumi
   3. Kirish hujumi

## Xizmatlardan voz kechishga undash hujumi

1. Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko’rsating.

## Ochiq kalitli shifrlar

* 1. Simmetrik shifrlar
  2. Oqimli shifrlar
  3. Blokli shifrlar

1. Jumlani to’ldiring. Simli va simsiz tarmoqlar orasidagi asosiy farq …
   1. Tarmoq chetki nuqtalari orasidagi xududning kengligi
   2. Himoyani amalga oshirish imkoniyati yo’qligi
   3. Himoya vositalarining chegaralanganligi

## Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlanmaydigan xudud mavjudligi

1. ERI da rad etish jarayoni - …
   1. Foydalanuvchi (B) qabul qilib olingan ma’lumotni o’zgartirib, shu

o’zgartirilgan ma’lumotni foydalanuvchi (A) yubordi deb ta’kidlaydi

* 1. (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

## Foydalanuvchi (A) foydalanuvchi (B) ga haqiqatdan ham ma’lumot jo’natgan bo’lib, uzatilgan ma’lumotni rad etishi mumkin

* 1. Foydalanuvchi (B) ning o’zi ma’lumot tayyorlab, bu soxta ma’lumotni foydalanuvchi (A) yubordi deb da’vo qiladi

1. Eng kam xarajatli zaxira nusxalash manzilini ko’rsating.
   1. O’sib boruvchi zaxiralash
   2. Bulutda zaxiralash

## Ichki zaxiralash

* 1. Tashqi zaxiralash

1. Jumlani to’ldiring. Ma’lumotni uzatishda kriptografik himoya …..

## Foydalanuvchanlik va butunlikni ta’minlaydi

* 1. Konfidensiallik va foydalanuvchanlikni ta’minlaydi
  2. Konfidensiallik va butunlikni ta’minlaydi
  3. Konfidensiallik ta’minlaydi

1. 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)

# L(03)

* 1. L(02)
  2. L(01)
  3. Berilgan shartlar yetarli emas

1. Qaysi himoya vositasi yetkazilgan axborotning butunligini tekshiradi?
   1. Router

## Virtual Private Network

* 1. Tarmoqlararo ekran
  2. Antivirus

1. Foydalanuvchini haqiqiyligini tekshirish jarayoni bu?
   1. Identifikatsiya
   2. Avtorizatsiya

## Autentifikatsiya

* 1. Ro’yxatga olish

1. Faqat foydalanishni boshqarish usullari keltirilgan javobni ko’rsating?

# DAC, MAC

* 1. ABAC, RSA
  2. RBAC, A5/1
  3. DAC, RSA

1. Belgilangan sharoitlarda tahdidning manbalarga potensial zarar yetkazilishini kutish bu?

## Risk

* 1. Tahdid
  2. Zaiflik
  3. Hujum

1. Quyidagilardan qaysi biri tarmoq xavfsizligi muammolariga sabab bo’lmaydi?
   1. Tug’ma texnologiya zaifligi

## Routerlardan foydalanmaslik

* 1. Tarmoqni xavfsiz bo’lmagan tarzda va zaif loyihalash
  2. Qurilma yoki dasturiy vositani noto’g’ri sozlanish

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

## Topologiya

* 1. Protokol
  2. Model

1. Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi?
   1. Ochiq kalit

## Dasturiy

* 1. Simmetrik
  2. Apparat

1. Tarmoq sathidagi VPN qaysi protokol asosida quriladi?
   1. L2F
   2. PPTP
   3. TLS

## IPSec

1. Qanday tahdidlar passiv hisoblanadi?
   1. Axborot xavfsizligini buzmaydigan tahdidlar
   2. Amalga oshishida axborot strukturasi va mazmunida hech narsani o’zgartirmaydigan tahdidlar
   3. Texnik vositalar bilan bog’liq bo’lgan tahdidlar
   4. Hech qachon amalga oshirilmaydigan tahdidlar
2. Jumlani to’ldiring. Hujumchi kabi fikrlash …. Kerak.

## Ma’lumot, axborot va tizimdan foydalanish uchun

* 1. Ma’lumotni aniq va ishonchli ekanligini bilish uchun
  2. Kafolatlangan amallarni ta’minlash uchun

1. Axborot xavfsizligida zaiflik bu?
   1. Tizim yoki tshkilotga zarar yetkazishi mumkin bo’lgan istalmagan hodisa
   2. Noaniqlikning maqsadlarga ta’siri
   3. Tashkilot uchun qadrli bo’lgan ixtiyoriy narsa

## Tahdidga sabab bo’luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson

1. Jumlani to’ldiring. Axborot xavfsizligiga bo’ladigan … tahdidlari maqsadli (atayin) tahdidlar deb ataladi.

## Foydalanuvchilar va xizmat ko’rsatuvchi hodimlarning hatoliklari

* 1. Tabiiy ofat va avariya
  2. Texnik vositalarning buzilishi va ishlamasligi
  3. Strukturalarni ruxsatsiz modifikatsiyalash

1. ushbu zaxiralash usuli tizim ishlamay turganda yoki

foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi. Ushbu usul zaxiralashning xavfsiz usuli hisoblanib, ma’lumotni nusxalash xavfidan himoyalaydi.

* 1. Issiq zaxiralash

## Sovuq zaxiralash

* 1. Iliq zaxiralash
  2. Ichki zaxiralash

1. OSI modelining quyi sathi bu?

## Fizik sath

* 1. Transport sathi
  2. Kanal sathi
  3. Tarmoq sathi

1. Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi bu?
   1. Tarmoq topologiyasi
   2. Kompyuter topologiyasi
   3. Tarmoq arxitekturasi

## Kompyuter tarmog’i

1. Hajmi bo’yicha eng kichik hisoblangan tarmoq turi bu –
   1. CAN

# PAN

* 1. MAN
  2. LAN

1. Tizimning turli resurslarga foydalanishni cheklash uchun foydalaniluvchi qoidalar to’plami haqidagi barcha narsalar bu?

## Avtorizatsiya

* 1. Autentifikatsiya
  2. Identifikatsiya
  3. Ruxsatlarni nazoratlash

1. Bir xil baroshlika ega bo’lganida quyidagi algoritmlardan qaysi birida kalit uzunligi eng kata bo’ladi?
   1. DES

# AES

* 1. A5/1
  2. RSA

1. 12 soni bilan o’zaro tub bo’lgan sonlarni ko’rsating.
   1. 14, 26
   2. 144, 4
   3. 12 dan tashqari barcha sonlar

## 11, 13

1. Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?

## Barcha javoblar to’g’ri

* 1. Boshqa kompyuterda yozib olingan ma’lumotlarni o’qishdan oldin har bir saqlagichni antivirus tekshiruvidan o’tkazish
  2. Kompyuterni zamonaviy antivirus darturiy vositasi bilan ta’minlash va uni doimiy yangilab boorish
  3. Faqat litsenziyali dasturiy ta’minotdan foydalanish

1. Kirish hujumlari bu?
   1. Foydalanuvchilarga va tashkilotlarda mavjud bo’lgan biror xizmatni cheklashga urinadi
   2. Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to’plashni maqsad qiladi

## Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi

* 1. Tarmoq haqida axborotni to’plash hujumchilarga mavjud

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

## 23

* 1. 21
  2. 22
  3. 19

1. Ochiq tarmoq yordamida himoyalangan tarmoqni qurish imkoniyatiga ega himoya vositasi bu?
   1. Antivirus
   2. Tarmoqlararo ekran

## Virtual Private Network

* 1. Router

1. Diskni shifrlash usuliga xos bo’lgan xususiyatlarni belgilang.
   1. Faqat kriptografik kalitlar xotirada saqlanib, shifrlangan fayllar ochiq holatda saqlanadi
   2. Asosiy fayl tizimining ustida joylashgan kriotografik fayl tizimidan foydalanish (masalan, ZSF, EncFS)

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

1. Jumlani to’ldiring. Autentifikatsiya tizimlari asoslanishiga ko’ra …. turga bo’linadi.

# A) 3

B) 5

C) 4

D) 2

1. Ikki kalitli kriptotizim bu –
   1. MAC tizimlari
   2. Simmetrik kriptotizim

## Ochiq kalitli kriptotizim

* 1. Xesh funksiyalar

1. Kriptologiya so’ziga berilgan to’g’ri tavsifni toping?
   1. Maxfiy shifrlarni buzish fani va san’ati
   2. Maxfiy shifrlarni yaratish fani va san’ati

## Maxfiy shifrlarni yaratish, buzish fani va san’ati

* 1. Axborotni himoyalash fani va san’ati

1. axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar

to’plami.

## Alifbo

* 1. Kodlash
  2. Shifrmatn
  3. Ochiq matn

1. Parollar 10 xonali uzunlikka va har bir xonasi uchun 14ta turli belgilar bo’lishi mumkin bo’lgan jami parollar soni nechta?
   1. 10^14

## 14^10

* 1. 140
  2. 24

1. Modul arifmetikasida mod9 bo’yicha 7 soniga teskari bo’lgan sonni toping?
   1. 7/9

## 4

* 1. 63
  2. 2

1. Paket filteri turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi?
   1. Ilova sathi parametrlari asosida
   2. Taqdimot sathi parametrlari asosida

## Tarmoq sathi parametrlari asosida

* 1. Kanal sathi parametrlari asosida

1. Kriptotizimning to’liq xavfsiz bo’lishi Kerxgovs prinsipiga ko’ra qaysi kattalikning nomalum bo’lishiga asoslanadi?
   1. Algoritm

## Kalit

* 1. Protokol
  2. Shifrmatn

1. RSA algoritmida p=3, q=11 bo’lsa, N sonidan kichik va u bilan o’zaro tub bo’lgan sonlar miqdorini ko’rsating.
   1. 43

## 20

* 1. 11
  2. 13

1. A5/1 algoritmidagi X registor uzunligi nechiga teng?
   1. 23

## 19

* 1. 18
  2. 22

1. Qaysi himoya vositasi tomonlarni autentifikatsiyalash imkoniyatini beradi?

## Virtual private network

* 1. Tarmoqlararo ekran
  2. Router
  3. Antivirus

1. Qaysi funksiya matnli fayllar bilan ishlashda mavjud put (joylashish) pozitsiyasini ifodalaydigan streampos turdagi qiymatni qaytaradi?
   1. Seekg()
   2. Seekp()
   3. Tellg()

## Tellp()

1. Foydalanuvchi yoki subyektni haqiqiyligini tekshirish jarayoni bu?

## Autentifikatsiya

* 1. Ruxsatlarni nazoratlash
  2. Avtorizatsiya
  3. Identifikatsiya

1. Foydalanuvchi parollari bazada qanday ko’rinishda saqlanadi?
   1. Bazada saqlanmaydi

## Xeshlangan ko’rinishda

* 1. Shifrlangan ko’rinishda
  2. Ochiq holatda

1. Qaysi bilim sohasi tashkil etuvchilar o’rtasidagi aloqani himoyalashga e’tibor qaratib, o’zida fizik va mantiqiy ulanishni birlashtiradi?
   1. Dasturiy ta’minotlar xavfsizligi
   2. Ma’lumotlar xavfsizligi

## Aloqa xavfsizligi

* 1. Tashkil etuvchilar xavfsizligi

1. Ruxsatsiz foydalanish, qo’pol kuch hujumi, imtiyozni orttirish, o’rtaga turgan odam hujumi, kabilar qaysi tarmoq xavfsizligiga kiritilgan hujumlar oilasiga tegishli?
   1. Razvedka hujumlari
   2. Zararli hujumlar
   3. Xizmatdan voz kechishga undash hujumlari

## Kirish hujumlari

1. Axborot xavfsizligida tahdid bu?
   1. Noaniqlikning maqsadlarga ta’siri
   2. Tashkilot uchun qadrli bo’lgan ixtiyoriy narsa

## Aktivga zarar yetkazishi mumkin bo’lgan istalmagan hodisa

* 1. U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz

1. Xavfsizlik bo’shlig’i bo’lib, turli foydalanuvchilarni autentifikatsiyalash usullarini aylanib o’tib hujumchiga tizimga kirish imkoniyatini taqdim etadi. Gap nima haqida bormoqda?

## Zaiflik

* 1. Aktiv
  2. Tahdid
  3. Hujum

1. Yaxlitlikni ta’minlash bu-?
   1. Ruxsatsiz bajarishdan himoyalash

## Ruxsatsiz yozishdan himoyalash

* 1. Ruxsatsiz o’qishdan himoyalash
  2. Ruxsat etilgan amallarni bajarish

1. Plastik kartadan to’lovni amalga oshirishda mavjud autentifikatsiya usuli qaysi sinfga tegishli?
   1. Bir faktorli autentifikatsiya

## Ikki faktorli autentifikatsiya

* 1. Tokenga asoslangan autentifikatsiya
  2. Biometrik autentifikatsiya

1. RAID 0 texnologiyasining vazifasi –
   1. Diskni navbatlanishi va xatolikni nazoratlash

## Diskni navbatlanishi

* 1. Bloklarni navbatlash va akslantirish
  2. Diskni akslantirish

1. Razvedka hujumlari bu?
   1. Tizimni fizik buzishni maqsad qiladi
   2. Foydalanuvchilarga va tashkilotlarga mavjud bo’lgan biror xizmatni cheklashga urinadi
   3. Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi

## Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to’plashni maqsad qiladi

1. Qaysi xususiyatlar RAID texnologiyasiga xos emas?
   1. Disklarni “qaynoq almashtirish” mumkin
   2. Xatoliklarni nazoratlash mumkin

## Shaxsiy kompyuterda foydalanish mumkin

* 1. Serverlarda foydalanish mumkin

1. Axborotni mavjudligini yashirish bilan shug’ullanuvchi fan sohasi bu –
   1. Kodlash

## Steganografiya

* 1. Kriptotahlil
  2. Kriptografiya

1. 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?
   1. Barcha javoblar to’g’ri

## Phishing

* 1. Protexting
  2. Spoofing

1. C=P XOR K – bir martali bloknotda shifrlash funksiyasi bo’lsa, unga mos deshifrlash funksiyasini ko’rsating? Bu yerda, P- ochiq kalit, K-kalit, C- shifrmatn
   1. P = C AND K
   2. P = C OR K

# P = C XOR K

* 1. P = C – K

1. Biror narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilari tushuniladi?
   1. Token, mashinaning kaliti
   2. Yuz tasviri, barmoq izi
   3. Biometrik parametrlar

## PIN, Parol

1. Qaysi biometrik parameter eng yuqori universallik xususiyatiga ega?
   1. Yuz tasviri

## Barmoq izi

* 1. Qo’l shakli
  2. Ko’z qorachig’i

1. Foydalanuvchi shaxsiy xabarlarni alohida shifrlashni unutgan vaqtlarda juda qo’l keladi. Gap qaysi shifrlash usuli xususida bormoqda?
   1. Apparat shifrlash
   2. Faylni shifrlash
   3. Dasturiy shifrlash

## Diskni shifrlash

1. Faktorlash muammosi asosida yaratilgan assimetrik shifrlash usuli.
   1. El-Gamal
   2. Elliptik egri chiziqga asoslangan shifrlash

# RSA

* 1. Diffi-Xelman

1. 64 ta belgidan iborat Sezar shifrlash usulida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin?
   1. 32
   2. 63!
   3. 32^2

## 63

1. “Yelka orqali qarash” hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan?
   1. Biometrik autentifikatsiya
   2. Tokenga asoslangan autentifikatsiya
   3. Ko’z qorachig’iga asoslangan autentifikatsiya

## Parolga asoslangan autentifikatsiya

1. Odatda mavjud bo’lgan IP – paket to’liq shifrlanib, unga yangi IP sarlavha beriladi. Ushbu amal qaysi himoya vositasida amalga oshiriladi?
   1. Antivirus vositasi

## Virtual xususiy tarmoq

* 1. Diskni shifrlash vositasi
  2. Tarmoqlararo ekran

1. Quyidagi ta’rif windows OTdagi qaysi hodisani tavsiflaydi?

Ma’lumotni yo’qotish yoki funksionallikni yo’qotish kabi muhim muammoni ko’rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, ……… hodisasi qayd etiladi.

* 1. Axborot
  2. Muvaffaqiyatli audit

## Xatolik

* 1. Ogohlantirish

1. Elektron ma’lumotlarni yo’q qilishda maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o’zgaririladigan usul bu ….
   1. Magnitsizlantirish

## Shredirlash

* 1. Yanchish
  2. Formatlash

1. Virus aniq bo’lganda va xususiyatlari aniq ajratilgan holatda eng katta samaradorlika ega zararli dasturni aniqlash usulini ko’rsating?
   1. Anomaliyaga asoslangan usul

## Signaturaga asoslangan usul

* 1. Barcha javoblar to’g’ri
  2. O’zgarishga asoslangan usul

1. O’zini yaxshi va foydali dasturiy vosita sifatida ko’rsatuvchi zararli dastur turi bu?
   1. Backdoors

## Troyan otlari

* 1. Adware
  2. Spyware

1. Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ….. amalga oshiriladi.
   1. Yashirish
   2. Kodlash

## Deshifrlash

* 1. Shifrlash

1. Jumlani to’ldiring. Tizimli fikrlash …. uchun kerak.
   1. Ma’lumot, axborot va tizimdan foydalanish

## Kafolatlangan amallarni ta’minlash

* 1. Ma’lumotni aniq va ishonchli ekanligini bilish
  2. Bo’lishi mumkin bo’lgan xavfni oldini olish

1. Ma’lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi?

## Zarur axborotni tanlashdan

* 1. Mos RAID sathini tanlashdan
  2. Mos zaxira nusxalash vositasini tanlashdan
  3. Mos zaxira nusxalash usulini tanlashdan

1. Operatsion tizimlarda keng qo’llaniluvchi foydalanishni boshqarish usuli bu?

# DAC

* 1. MAC
  2. RBAC
  3. ABAC

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

## Ilova, taqdimot va seans

* 1. Ilova
  2. Ilova va taqdimot
  3. Seans va taqdimot

1. Yaratilishi uchun faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmi nomini ko’rsating?
   1. DES
   2. El-Gamal
   3. A5/1

# RSA

1. Shaxsiy simsiz tarmoqlar qo’llanilish sohasini belgilang.

## Tashqi qurilmalar kabellaring o’rnida

* 1. Binolar va korxonalar va internet orasida belgilangan simsiz bog’lanish
  2. Butun dunyo bo’yicha internetdan foydalanishda
  3. Simli tarmoqlarni mobil kengaytirish

1. 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.
   1. ABAC

# MAC

* 1. RMAC
  2. DAC

1. Qaysi bilim sohasi foydalanilayotgan tizim yoki axborot xavfsizligini

ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi?

* 1. Tashkil etuvchilar xavfsizligi
  2. Ma’lumotlar xavfsizligi

## Dasturiy ta’minotlar xavfsizligi

* 1. Aloqa xafsizligi

1. RSA algoritmida p=5 q=13 e=7 ga teng bo’lsa, shaxsiy kalitni hisoblang?

## 7

* 1. 65
  2. 35
  3. 13

1. DNS serverlari tarmoqda qanday vazifani amalga oshiradi?
   1. Tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq uchun chiqish nuqtasi vazifasini bajaradi
   2. Internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlash funksiyasini amalga oshiradi
   3. Ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq uchun kiruvchi nuqta vazifasini bajaradi

## Xost nomlari va internet nomlarini IP manzillarga o’zgartirish va teskarisini amalga oshiradi

1. VPNning texnik amalga oshirilishiga ko’ra turlari keltirilgan qatorni toping.
2. Kanal sathidagi VPN; tarmoq sathidagi VPN; seans sathidagi VPN

## Dasturiy ko’rinishdagi VPN; maxsus shifrlash protsessoriga ega apparat vosita ko’rinishidagi VPN

1. Marshuritizator ko’rinishidagi VPN; tarmoqlararo ko’rinishidagi VPN

E) Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN

1. Quyidagilardan qaysilari tarmoq topologiyalari hisoblanadi?

## Halqa, yulduz, shina, daraxt

* 1. UDP, TCP/IP, FTP
  2. SMTP, HTTP, UDP
  3. OSI, TCP/IP

1. Jumlani to’ldiring. Parol kalitdan ….. farq qiladi.
   1. Uzunligi bilan
   2. Tasodifiylik darajasi bilan

## Belgilari bilan

* 1. Samaradorligi bilan

1. Portlarni va operatsion tizimni skanerlash razvedka hujumlarining qaysi turida amalga oshiriladi?
   1. Passiv
   2. Lug’atga asoslangan
   3. DNS izi

## Aktiv

Axborot xavfsizligining asosiy maqsadlaridan biri-bu…==== Obyektga bevosita ta’sir qilish====

#Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish==== Axborotlarni shifrlash, saqlash, yetkazib berish====

Tarmoqdagi foydalanuvchilarni xavfsizligini ta’minlab berish

++++

Windows OTda necha turdagi hodisa ro‘yxatga olinadi?==== #5 ta====

2 ta====

3 ta====

4 ta

++++

Konfidentsiallikga to‘g‘ri ta’rif keltiring.====

#axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; ==== axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati; ====

axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati; ==== axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati;

++++

Kriptografiya faninining asosiy maqsadi nima? ==== #maxfiylik, yaxlitlilikni ta’minlash====

ishonchlilik, butunlilikni ta’minlash==== autentifikatsiya, identifikatsiya==== ma’lumotlarni shaklini o‘zgartish

++++

Kriptografiyada kalitning vazifasi nima? ==== Bir qancha kalitlar yig‘indisi====

#Matnni shifrlash va shifrini ochish uchun kerakli axborot==== Axborotli kalitlar to‘plami====

Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

++++

Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq? ==== #simmetrik kriptotizimlar====

assimetrik kriptotizimlar==== ochiq kalitli kriptotizimlar==== autentifikatsiyalash

++++

Autentifikatsiya nima? ====

#Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi====

Tizim me’yoriy va g‘ayritabiiy hollarda rejalashtirilgandek o‘zini tutishligi holati==== Istalgan vaqtda dastur majmuasining mumkinligini kafolati====

Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi

++++

Identifikatsiya bu- …====

#Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni==== Ishonchliligini tarqalishi mumkin emasligi kafolati====

Axborot boshlang‘ich ko‘rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o‘zgarishlar====

Axborotni butunligini saqlab qolgan holda uni elementlarini o‘zgartirishga yo‘l qo‘ymaslik

++++

Kriptobardoshlilik deb nimaga aytilladi? ====

#kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi==== axborotni qayta akslantirib himoyalash muammosi bilan shug‘ullanadi====

kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi====

axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

++++

Kriptografiyada matn –bu.. ====

#alifbo elementlarining tartiblangan to‘plami====

matnni shifrlash va shifrini ochish uchun kerakli axborot====

axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam==== kalit axborotni shifrlovchi kalitlar

++++

Kriptotizimga qo‘yiladigan umumiy talablardan biri nima? ==== #shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak====

shifrlash algoritmining tarkibiy elementlarini o‘zgartirish imkoniyati bo‘lishi lozim==== ketma-ket qo‘llaniladigan kalitlar o‘rtasida oddiy va oson bog‘liqlik bo‘lishi kerak==== maxfiylik o‘ta yuqori darajada bo‘lmoqligi lozim

++++

Berilgan ta’riflardan qaysi biri assimetrikrik tizimlarga xos? ====

#Assimetrikrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi====

Assimetrikrik tizimlarda k1=k2 bo‘ladi, ya’ni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi====

Assimetrikrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma’lum bo‘ladi, ochiq kalitni esa faqat qabul qiluvchi biladi====

Assimetrikrik kriptotizimlarda k1≠k2 bo‘lib, kalitlar hammaga oshkor etiladi

++++

Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…====

#login==== parol====

identifikatsiya==== token

++++

Uning egasi haqiqiyligini aniqlash jarayonida matnhiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima? ====

#parol==== login==== identifikatsiya==== maxfiy maydon

++++

Ro‘yxatdan o‘tish-bu…====

#foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni====

axborot tizimlari ob’yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo‘yicha solishtirib uni aniqlash jarayoni====

obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketma- ketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash====

foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

++++

Axborot qanday sifatlarga ega bo‘lishi kerak? ==== #ishonchli, qimmatli va to‘liq====

uzluksiz va uzlukli====

ishonchli, qimmatli va uzlukli==== ishonchli, qimmatli va uzluksiz

++++

Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish nima deb ataladi?==== sirli yozuv====

#steganografiya==== skrembler====

shifr mashinalar

++++

Kriptografiya fan sifatida shakllanishida nechta davrlarga bo‘linadi?==== #4 ga====

3 ga====

2 ga====

5 ga

++++

Shifrmatntni ochiq matntga akslantirish jarayoni nima deb ataladi? ==== #Deshifrlash====

Xabar==== Shifrlangan xabar==== Shifrlash

++++

Risk-tushunchasi nima? ====

#Belgilangan sharoitda tahdidning manbalarga bo‘lishi mumkin bo‘lgan zarar yetkazilishini kutish ====

Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan ==== Shifrmatntni ochiq matntga akslantirish jarayoni ==== Kalitlarni generatsiya qilish usuli

++++

Tahdid-tushunchasi nima? ====

#Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa==== Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa====

Bu riskni o‘zgartiradigan harakatlar====

Bu noaniqlikning maqsadlarga ta’siri

++++

Kodlash terminiga berilgan ta’rifni belgilang.====

#Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir====

Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi====

Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi====

Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi

++++

Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug‘ullanadi? ==== Kartografiya====

#Kriptoanaliz==== Kriptologiya==== Adamar usuli

++++

Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi? ==== #{d, n} – yopiq, {e, n} – ochiq; ====

{d, e} – ochiq, {e, n} – yopiq; ====

{e, n} – yopiq, {d, n} – ochiq; ====

{e, n} – ochiq, {d, n} – yopiq;

++++

Zamonaviy kriptografiya qanday bo‘limlardan iborat? ====

#Simmetrik kriptotizimlar; Ochiq kalitli kriptotizimlar; Elektron raqamli imzo; Kalitlarni boshqarish ====

Elektron raqamli imzo; Kalitlarni boshqarish, Sertifikatlash, Shifrlash;====

Simmetrik kriptotizimlar; Ochiq kalitli kriptotizimlar; ====

Simmetrik kriptotizimlar; Ochiq kalitli kriptotizimlar; Kalitlarni yaratish, Litsenziyalsh;

++++

Shifr nima?====

#Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm ====

Kalitlarni taqsimlash usuli==== Kalitlarni boshqarish usuli ==== Kalitlarni generatsiya qilish usuli

++++

Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? ====

Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi====

#Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi====

Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin==== Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat deshifrlash mumkin

++++

Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi? ==== Simmetrik algoritmlar====

Assimmetrik algoritmlar==== #Xesh funksiyalar==== Kodlash

++++

Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu... ====

#Avtorizatsiya==== Shifrlash====

Identifikatsiya==== Autentifikatsiya

++++

Autentifikatsiya faktorlari nechta? ==== 4 ta====

#3 ta====

5 ta====

6 ta

++++

Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

====

#Biometrik autentifikatsiya==== Biron nimaga egalik asosida==== Biron nimani bilish asosida==== Parolga asoslangan

++++

Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini belgilaydigan atamani toping.====

Shifr matn uzunligi==== #Kriptobardoshlik==== Shifrlash algoritmi==== Texnika va texnologiyalar

++++

Qog‘oz ma’lumotlarni yo‘q qilish odatda necha xil usuldan foydalaniladi? ==== #4 xil====

8 xil====

7 xil====

5 xil

++++

Kiberjinoyat qanday turlarga bo‘linadi?==== #Ichki va tashqi====

Faol va passiv==== Asosiy va quyi==== Xalqaro va milliy

++++

“Kiberxavfsizlik to‘g‘risida” Qonun qachon tasdiqlangan?==== #15.04.2022 y====

20.03.2021 y====

02.01.2000 y====

15.01.1995 y

++++

Kiberjinoyatchilik bu –. . . ====

#Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. ====

Kompyuter o‘yinlari====

Faqat banklardan pul o‘g‘irlanishi==== Autentifikatsiya jarayonini buzish

++++

Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?

====

Axborotdan ruhsatsiz foydalanish==== Zararkunanda dasturlar====

An’anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili==== #Texnik vositalarning buzilishi va ishlamasligi

++++

Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi? ====

Axborotning konfedentsialligi==== Foydalanuvchanligi====

#Ma’lumotlar butunligi==== Ixchamligi

++++

Biometrik autentifikatsiyalashning avfzalliklari-bu: ==== Bir marta ishlatilishi====

#Biometrik parametrlarning noyobligi==== Biometrik parametrlarni o‘zgartirish imkoniyati==== Autentifikatsiyalash jarayonining soddaligi

++++

Simmetrik shifrlashning noqulayligi – bu: ==== #Maxfiy kalitlar bilan ayirboshlash zaruriyatidir==== Kalitlar maxfiyligi====

Kalitlar uzunligi====

Shifrlashga ko‘p vaqt sarflanishi va ko'p yuklanishi

++++

Token, smartkartalarda xavfsizlik tomonidan kamchiligi nimada? ==== Foydalanish davrida maxfiylik kamayib boradi====

Qurilmalarni ishlab chiqarish murakkab jarayon==== #Qurilmani yo'qotilishi katta xavf olib kelishi mumkin==== Qurilmani qalbakilashtirish oson

++++

Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating====

Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi==== #Zilzila, yong‘in, suv toshqini va hak. ====

Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi====

Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani

++++

Ma’lumotlarni tasodifiy sabablar tufayli yo‘qolish sababini belgilang====

#Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi====

Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi====

Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. ====

Zilzila, yong‘in, suv toshqini va hak.

++++

Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang. ==== Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi. ====

#Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. ====

Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi==== Zilzila, yong‘in, suv toshqini va hak.

++++

"Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat? ==== Parolni esda saqlash kerak bo'ladi. ====

Parolni almashtirish jarayoni murakkabligi==== Parol uzunligi soni cheklangan==== #Foydalanish davrida maxfiylik kamayib boradi

++++

Nima uchun autentifikatsiyalashda parol ko‘p qo‘llaniladi? ==== #Sarf xarajati kam, almashtirish oson====

Parolni foydalanubchi ishlab chiqadi==== Parolni o‘g‘rishlash qiyin====

Serverda parollar saqlanmaydi

++++

Elektron xujjatlarni yo‘q qilish usullari qaysilar? ==== Yoqish, ko‘mish, yanchish====

#Shredirlash, magnitsizlantirish, yanchish==== Shredirlash, yoqish, ko‘mish====

Kimyoviy usul, yoqish.

++++

Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan? ==== 4 taga====

2 taga====

5 taga====

#3 taga

++++

Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi? ==== #Knx1@8&h ====

qwertyu==== salomDunyo==== Mashina505

++++

Parollash siyosatiga ko'ra parol tanlash shartlari qanday? ==== Kamida 7 belgi; katta va kichik xavflar, sonlar qo'llanishi kerak. ====

#Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak.

====

Kamida 6 belgi; katta xarflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. ==== Kamida 6 belgi; katta va kichik xarflar, kamida bitta maxsus simvol qo'llanishi kerak.

++++

MD5, SHA1, SHA256, O‘z DSt 1106:2009- qanday algoritmlar deb ataladi? ==== Kodlash====

#Xeshlash==== Shifrlash==== Stenografiya

++++

Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

====

O‘rta asr davrida==== 15 asr davrida====

#1-2 jahon urushu davri==== 21 asr davrida

++++

"Fishing" tushunchasi-bu…:====

Kompyuter va kompyuter tarmoqlarida odamlarning etikasi==== Kompyuter, dasturlar va tarmoqlar xavfsizligi====

#Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet- hujumi====

Kompyuter tizimlariga ruxsatsiz ta’sir ko'rsatish

++++

Axborot xavfsizligi boshqaruv tizimida "Aktiv" so'zi nimani anglatadi?====

Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyot.====

Hisoblash tizimi xizmatlaridan foydalanish huqu kiberxavfsizlik qiga ega shaxs (shaxslar guruxi, tashkilot).====

#Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar====

Ma’lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo'ljallangan dasturiy va apparat vositalar

++++

Axborot xavfsizligi timsollarini ko'rsating.==== Haker, Krakker====

#Alisa, Bob, Eva==== Buzg'unchi, hujumchi==== subyekt, user

++++

Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.==== #Qonunlar====

Qarorlar==== Standartlar==== Farmonlar

++++

Qaysi siyosat tizim resurslarini foydalanishda hech qanday cheklovlar qo'ymaydi?==== Ruxsat berishga asoslangan siyosat====

Paranoid siyosat==== Extiyotkorlik siyosati==== #Nomuntazam siyosat

++++

“Hаmmа nаrsа tа’qiqlаnаdi.” Bu qаysi xаvfsizlik siyosаtigа xos?==== Ruxsаt berishgа аsoslаngаn siyosаt (Permissive Policy)====

#Pаrаnoid siyosаti (Pаrаnoid Policy)==== Ehtiyotkorlik siyosаti (Prudent Policy)==== Nomuntаzаm siyosаt (Promiscuous Policy

++++

Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…====

Kibersport deb ataladi==== Kiberterror deb ataladi==== #Kiberjinoyat deb ataladi==== Hakerlar uyushmasi deyiladi

++++

Qaysi siyosat turli hisoblash resurslaridan to'g'ri foydalanishni belgilaydi?==== #Maqbul foydalanish siyosati====

Paranoid siyosat====

Ruxsat berishga asoslangan siyosat==== Nomuntazam siyosat

++++

Qaysi siyosatda Adminstrator xavfsiz va zarur xizmatlarga indvidual ravishda ruxsat beradi?==== Paranoid siyosat====

Ruxsat berishga asoslangan siyosat==== Nomuntazam siyosat==== #Extiyotkorlik siyosati

++++

Qaysi siyosatga ko'ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?==== Nomuntazam siyosat====

Paranoid siyosat====

#Ruxsat berishga asoslangan siyosat====

Extiyotkorlik siyosati

++++

Qaysi siyosatga ko'ra hamma narsa taqiqlanadi?==== Ruxsat berishga asoslangan siyosat==== Nomuntazam siyosat====

Extiyotkorlik siyosati==== #Paranoid siyosat

++++

Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to'plami nima deyiladi?====

#Xavfsizlik siyosat==== Standart==== Qaror====

Buyruq

++++

Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to'liq tasavvurga ega shaxs kim deb ataladi?====

Xavfsizlik mutaxasisi==== Rahbar==== Foydalanuvchi==== #Xavfsizlik ma'muri (admin)

++++

Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o‘z ichiga oladi?==== #Xalqaro va milliy huquqiy me’yorlarni====

Tashkiliy va xalqaro me’yorlarni==== Ananaviy va korporativ me’yorlarni==== Davlat va nodavlat tashkilotlari me’yorlarni

++++

Ehtiyotkorlik siyosati (Prudent Policy) – bu ….====

Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi==== Hamma narsa ta’qiqlanadi====

Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi==== #Barcha hizmatlar blokirovka qilingandan so‘ng bog’lanadi

++++

... - faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot. ====

#Parol ==== Login==== Maxfiy kalit ====

Shifrlangan axborot

++++

“Dasturiy ta’minotlar xavfsizligi” bilim sohasi - bu ... ====

#foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi. ====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi. ====

tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi. ====

kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

++++

“Jamoat xavfsizligi” bilim sohasi - bu … ====

#u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi. ====

tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini====

foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

++++

“Ma’lumotlar xavfsizligi” bilim sohasi - bu …====

#ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.====

foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.====

tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

++++

“Tizim xavfsizligi” bilim sohasi - bu …====

#tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi.====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.====

tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.====

kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

++++

“Xodim xavfsizligi” tushunchasi- bu…====

#Qandaydir jiddiy axborotdan foydalanish imkoniyatiga ega barcha xodimlarning kerakli avtorizatsiyaga va barcha kerakli ruxsatnomalarga egalik kafolatini ta’minlovchi usul.====

Axborot tarmog'ini ruxsatsiz foydalanishdan, me’yoriy harakatiga tasodifan aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.====

Destruktiv harakatlarga va yolg'on axborotni zo'rlab qabul qilinishiga olib keluvchi ishlanadigan va saqlanuvchi axborotdan ruxsatsiz foydalanishga urinishlarga kompyuter tizimining qarshi tura olish hususiyati.====

Korxona o'z faoliyatini buzilishsiz va to'xtalishsiz yurgiza oladigan vaqt bo'yicha barqaror bashoratlanuvchi atrof-muhit holati.

++++

“Yaxlitlik” atamasiga berilgan ta’rifni belgilang.====

#Bu yozilgan va xabar qilingan ma’luotlarning haqiqiyligini, to‘g’riligini, butunligini saqlash qobiliyati====

Funksionala imkoniyatni o‘z vaqtida foydalanish====

Tizimning ruxsat berilgan foydalanish uchun ma’lumot tarqatishni cheklash====

Korxona o'z faoliyatini buzilishsiz va to'xtalishsiz yurgiza oladigan vaqt bo'yicha barqaror bashoratlanuvchi atrof-muhit holati

++++

……–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.====

#Kiberxavfsizlik==== Axborot xavfsizligi==== Kiberjtnoyatchilik==== Risklar

++++

Assimetrikrik kriptotizimlarda axborotni shifrlashda va deshifrlash uchun qanday kalit ishlatiladi? ====

#Ikkita kalit: ochiq va yopiq==== Bitta kalit====

Elektron raqamli imzo==== Foydalanuvchi identifikatori

++++

Autentifikatsiya jarayoni qanday jarayon? ====

#obyekt yoki subyektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketma- ketligidan iborat maxfiy axborotni tekshirish orqali asilligini aniqlash====

axborot tizimlari obyekt va subyektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo‘yicha solishtirib uni aniqlash jarayoni====

foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni====

foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni

++++

Avtorizatsiya nima? ====

#Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilarga tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni====

Subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim qilish jarayoni====

Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni====

Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilar

++++

Axborot o‘lchovini kamayish tartibini to‘g’ri tanlang==== #Terabayt,gigabayt,megabayt==== Bit,bayt,kilobayt,megabayt==== Gigabayt,megabayt,bayt==== Gigabayt,megabayat,terobayt

++++

Axborot o‘lchovini o‘sish tartibini to‘g’ri tanlang==== #Kilobayt,megabayt,gigabayt==== Bit,bayt,megabayt,kilobayt==== Gigabayt,megabayt,pikobayt==== Gigabayt,terabayt,pikobayt

++++

Axborot xavfsizligi qanday asosiy xarakteristikalarga ega? ==== #Butunlik, konfidentsiallik, foydalanuvchanlik====

Butunlik, himoya, ishonchlilikni o’rganib chiqishlilik==== Konfidentsiallik, foydalana olishlik==== Himoyalanganlik, ishonchlilik, butunlik

++++

Axborot xavfsizligining huquqiy ta'minotiga nimalar kiradi? ====

#Qonunlar, aktlar, me'yoriy-huquqiy hujjatlar, qoidalar, yo'riqnomalar, qo'llanmalar majmui====

Qoidalar yo'riqnomalar, tizim arxetikturasi, xodimlar malakasi, yangi qoidalar, yangi yo'riqnomalar, qo'llanmalar majmui====

Qoidalar, yo'riqnomalar, tizim strukturasi, dasturiy ta’minot==== Himoya tizimini loyihalash, nazorat usullari

++++

"Barcha xizmatlar blokirovka qilingandan so‘ng bog’lanadi". -Bu qaysi xavfsizlik siyosatiga hos?

====

#Ehtiyotkorlik siyosati (Prudent Policy)==== Nomuntazam siyosat (Promiscuous Policy) ==== Paranoid siyosati (Paranoid Policy) ====

Ruxsat berishga asoslangan siyosat (Permissive Policy)

++++

Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo‘linadi? ==== #Blokli va oqimli====

DES va oqimli==== Feystel va Verman==== SP− tarmoq va IP

++++

BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? ==== #AES, Serpent, Twofish====

Pleyfer, Sezar====

DES, sezar, Futurama ====

AES, Serpent, Twofish, Triple DES, GOST 28147-89

++++

Blokli shifrlash tushunchasi nima? ====

#shifrlanadigan matn blokiga qo‘llaniladigan asosiy akslantirish==== murakkab bo‘lmagan kriptografik akslantirish====

axborot simvollarini boshqa alfavit simvollari bilan almashtirish==== ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi

++++

Elektron pochtaga kirishda foydalanuvchi qanday autetntifikasiyalashdan o‘tadi? ==== #Parol asosida====

Smart karta asosida==== Biometrik asosida==== Ikki tomonlama

++++

Elektron raqamli imzo - bu …====

#xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimcha==== matnni shifrlash va shifrini ochish uchun kerakli axborot====

axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam==== kalit axborotni shifrlovchi kalitlar

++++

Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? ==== #Imzo qo‘yish va imzoni tekshirishdan====

Faqat imzo qo‘yishdan==== Faqat imzoni tekshirishdan==== Kalitlarni taqsimlashdan

++++

Elektron raqamli imzo kalitlari ro'yxatga olish qaysi tashkilot tomonidan bajariladi==== #Sertifikatlari roʻyxatga olish markazlari====

Tegishli Vazirliklar====

Axborot xavfsizligi markazlari==== Davlat Hokimiyati

++++

Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima? ====

#Autentifikatsiya ==== Identifikatsiya ==== Avtorizatsiya ==== Ma’murlash

++++

Kriptografiyada kalit – bu …====

#Matnni shifrlash va shifrini ochish uchun kerakli axborot==== Bir qancha kalitlar yig’indisi====

Axborotli kalitlar to‘plami====

Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

++++

Kiberetika tushunchasi-bu…====

#Kompyuter va kompyuter tarmoqlarida odamlarning etikasi====

Kompyuter, dasturlar va tarmoqlar xavfsizligi==== Kompyuter tizimlariga ruxsatsiz ta’sir ko'rsatish====

Tashkilot va odamlarning mahsus va shahsiy ma’lumotlarini olishka qaratilgan internet-atakasi

++++

Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi? ====

#tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi ==== tashkilot xodimlari himoyasini ta’minlaydi ====

tashkilot axborotlari va binolarining himoyasini ta’minlaydi ==== tashkilot omborini va axborotlari himoyasini ta’minlaydi

++++

Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda qo'llaniladi? ====

#ochiq kalitlar==== yopiq kalitlar==== seans kalitlari==== Barcha tutdagi kalitlar

++++

Kriptografiyada "alifbo" deganda nima tushuniladi? ====

#axborotni ifodalashda ishlatiluvchi bilgilarning chekli to‘plami tushuniladi ==== matnni shifrlash va shifrini ochish uchun kerakli axborot====

xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimcha==== alfavit elementlaridan tartiblangan nabor

++++

O’zbekistonda masofadan elektron raqamli imzo olish uchun qaysi internet manzilga murojaat qilinadi? ====

#e-imzo.uz==== elektron-imzo.uz====

imzo.uz==== eri.uz

++++

Oqimli shifrlashning mohiyati nimada? ====

#Oqimli shifrlash birinchi navbatda axborotni bloklarga bo‘lishning imkoni bo‘lmagan hollarda zarur, ====

Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo‘natish uchun oqimli shifrlash zarur, ====

Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo‘yicha shifrlaydi====

Oqimli shifrlash birinchi navbatda axborotni bloklarga bo‘lishning imkoni bo‘lgan hollarda zarur,

++++

RSA algoritmi qanday jarayonlardan tashkil topgan? ==== #Kalitni generatsiyalash; Shifrlash; Deshifrlash. ==== Shifrlash; Imzoni tekshirish; Deshifrlash====

Kalitni generatsiyalash; imzolash; Deshifrlash. ==== Imzoni tekshirish ; Shifrlash; Deshifrlash.

++++

Shaxsning, o‘zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, axborot-kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu? ====

#login==== parol==== identifikatsiya==== maxfiy maydon

++++

Shifrlash qanday jarayon? ====

#akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi==== kalit asosida shifrmatn ochiq matnga akslantiriladi====

shifrlashga teskari jarayon====

almashtirish jarayoni bo‘lib: ochiq matn deb nomlanadigan matn o‘girilgan holatga almashtiriladi

++++

Kichik xajmdagi xotira va hisoblash imkoniyatiga ega bo‘lgan, o‘zida parol yoki kalitni saqlovchi qurilma nima deb ataladi? ====

#Token, Smartkarta ==== Chip ====

Fleshka ==== Disk

++++

Cisco tashkiloti “kiberxavfsizlik” atamasiga qanday ta’rif bergan?====

#Kiberxavfsizlik - tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti====

Hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan

====

Bu yozilgan va xabar qilingan ma’luotlarning haqiqiyligini, to’g’riligini, butunligini saqlash qobiliyati====

Ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.

++++

Foydalanuvchanlik-bu…====

#avtorizatsiyalangan mantiqiy obyekt so‘rovi bo‘yicha axborotning tayyorlik va foydalanuvchanlik holatida bo‘lishi xususiyati====

axborotning buzilmagan ko‘rinishida (axborotning qandaydir qayd etilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati====

axborot yoki uni eltuvchisining shunday holatiki, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi====

potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi

++++

Kiberxavfsizlik bilim sohasi nechta bilim sohasini o’z ichiga oladi?==== #8 ta====

7 ta====

6 ta====

5 ta

++++

Ijtimoiy (sotsial) injineriya-bu…====

#turli psixologik usullar va firibgarlik amaliyotining to‘plami, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olish====

Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish====

axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi====

foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

++++

Kiberxavfsizlik arxitekturasi nechta sathga ajratiladi?==== #3ta====

2 ta====

4 ta====

5 ta

++++

Tashkilot axborot xavfsizligi siyosati-bu…====

#mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. ====

bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. ====

mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi. ====

mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

++++

Muammoga qaratilgan xavfsizlik siyosatlari …====

mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. ====

#bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. ====

mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi. ====

mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

++++

Tizimga qaratilgan xavfsizlik siyosatlari …====

mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. ====

bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. ====

#mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi. ====

mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

++++

Internetdan foydalanish siyosati. …====

mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. ====

bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. ====

mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi. ====

#mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

++++

Ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o‘zgartirishlar oilasi-…====

#Kriptotizim==== Deshifrlash==== Rasshifrovkalash==== Shifrlash

++++

O‘zgartirishlar oilasidan birini tanlashni ta’minlovchi kriptografik algoritmning qandaydir parametrlarining muayyan qiymati-…====

Kriptotizim==== #Kalit==== Rasshifrovkalash==== Shifrlash

++++

"Axborot olish va kafolatlari va erkinligi to'g'risda"gi Qonuning maqsadi nimadan iborat?====

#Har kimning axborotni erkin va moneliksiz izlash, olish, tadqiq etish, uzatish hamda tarqatishga doir konstitutsiyaviy huquqini amalga oshirish jarayonida yuzaga keladigan munosabatlarni tartibga solish====

Axborotlarni maxfiylashtirish va maxfiylikdan chiqarish ushbu Qonunga hamda o'zbekiston Respublikasi Vazirlar Mahkamasi tasdiqlaydigan ma’lumotlarning maxfiylik darajasini aniqlash va belgilash ====

Shaxsga doir ma’lumotlar sohasidagi munosabatlarni tartibga solish.====

Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.

++++

"Axborotlashtirish to'g'risida"gi Qonunning maqsadi nimadan iborat?====

#Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.====

Shaxsga doir ma’lumotlar sohasidagi munosabatlarni tartibga solish.====

Har kimning axborotni erkin va moneliksiz izlash, olish, tadqiq etish, uzatish hamda tarqatishga doir konstitutsiyaviy huquqini amalga oshirish jarayonida yuzaga keladigan munosabatlarni tartibga solish====

Axborotlarni maxfiylashtirish va maxfiylikdan chiqarish ushbu Qonunga hamda o'zbekiston Respublikasi Vazirlar Mahkamasi tasdiqlaydigan ma’lumotlarning maxfiylik darajasini aniqlash va belgilash

++++

"Backdoors"-qanday zararli dastur?====

#zararli dasturiy kodlar bo'lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o'tib tizimga kirish imkonini beradi, masalan, administrator parolisiz imtiyozga ega bo'lish====

foydalanuvchi ma’lumotlarini qo'lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod====

ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi====

marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi dasturiy ta’minot

++++

.... – o‘zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma’lumoti va xavfsizlik algoritmlarini saqlaydi.====

#Sim karta ==== Token ==== Smart karta ====

Elektron raqamli imzo

++++

.... kompyuter tarmoqlari bo‘yicha tarqalib, kompyuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o‘zining nusxasini qoldiradi.====

#“Chuvalchang” va replikatorli virus==== Kvazivirus va troyan virus====

Troyan dasturi==== Mantiqiy bomba

++++

“Aloqa xavfsizligi” bilim sohasi - bu …====

#tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.====

foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.====

kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

++++

“Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?==== #Foydalanishni boshqarish====

Tarmoqni loyihalash==== Foydalanish==== Identifikatsiya

++++

“Inson xavfsizligi” bilim sohasi - bu …====

#kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi====

tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.====

foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi

++++

“Tashkil etuvchilar xavfsizligi” - bu …====

#katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi====

foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi====

tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi====

kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi

++++

“Tashkilot xavfsizligi” bilim sohasi - bu …====

#tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini====

foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi====

tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi

++++

…. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.==== #UDP====

HTTP==== TCP==== FTP

++++

….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.====

#TCP==== IP==== HTTP==== FTP

++++

Access control list va Capability list bu nimaning asosiy elementi hisoblanadi?==== #Lampson matritsasining====

XASML standartining ====

Role-based access control RBACning==== Attribute based access control (ABAC)ning

++++

“Adware” zararli dastur xususiyati nimadan iborat?====

#marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi dasturiy ta’minot.====

foydalanuvchi ma’lumotlarini qo'lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.====

bir qarashda yaxshi va foydali kabi ko'rinuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi.====

o'zini o'zi ko'paytiradigan programma bo'lib, o'zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi

++++

Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?====

#"Issiq zaxiralash"==== "Sovuq saxiralash"==== "Iliq saxiralash"==== "To'liq zaxiralash"

++++

Qaysi zaxiralash usuli offlayn zaxiralash deb ham atalib, tizim ishlamay turganida yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi?====

#"Sovuq saxiralash"==== "Issiq zaxiralash"==== "Iliq saxiralash"==== "To'liq zaxiralash"

++++

Qaysi zaxiralashda tizim muntazam yangilanishni amalga oshirish uchun tarmoqqa bog‘lanishi kerak bo‘ladi?====

#"Iliq saxiralash"==== "Sovuq saxiralash"==== "Issiq zaxiralash"==== "To'liq zaxiralash"

++++

Agar RSA algotirmida e-ochiq kalitni, d-maxfiy kalitni, n-modul ifodalasa, qaysi formula deshifrlashni ifodalaydi?====

#M = C^d mod n; ==== C = M^d mod n; ====

C = M^ed mod n; ==== M = C^e mod n;

++++

Agar RSA algotirmida e-ochiq kalitni, d-maxfiy kalitni, n-modul , qaysi formula shifrlashni ifodalaydi? ====

#C = M^e mod n; ==== C = M^d mod n; ====

C = M^ed mod n; ==== M = C^e mod n;

++++

Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...

====

#Tamoqlararo ekranlarning o‘rnatilishi==== Tashkiliy ishlarni bajarilishi====

Globol tarmoqdan uzib qo‘yish====

Aloqa kanallarida optik toladan foydalanish

++++

Akslantirish tushunchasi deb nimaga aytiladi? ====

#1-to‘plamli elementlariga 2-to‘plam elementalriga mos bo‘lishiga====

1-to‘plamli elementlariga 2-to‘plam elementalrini qarama-qarshiligiga==== har bir elementni o‘ziga ko‘payimasiga====

agar birinchi va ikinchi to‘plam bir qiymatga ega bo‘lmasa

++++

Antivirus dasturiy vositalari viruslarni tahlil qilishiga ko'ra necha turga bo'linadi? ==== #2 turga fayl signaturaga va tahlilga asoslangan====

2 turga faol va passiv==== 2 turga pulli va pulsiz==== 2 turga litsenziyali va ochiq

++++

Antivirus dasturlarini ko‘rsating. ==== #Drweb, Nod32, Kaspersky====

arj, rar, pkzip, pkunzip====

winrar, winzip, winarj==== pak, lha

++++

Antiviruslar viruslarni asosan qanday usulda aniqlaydi? ==== #Signaturaga asoslangan====

Anomaliyaga asoslangan==== O‘zgarishni aniqlashga asoslangan==== Defragmentatsiya qilish

++++

Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud. ==== #detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar==== detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar==== vaktsinalar, privivkalar, revizorlar, matnhiruvchilar====

privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar

++++

AQShning axborotni shifrlash standartini keltirilgan javobni ko‘rsating? ==== #DES(Data Encryption Standart) ====

RSA (Rivest, Shamir ва Adleman) ==== AES (Advanced Encryption Standart) ==== Aniq standart ishlatilmaydi

++++

Assimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? ====

#shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun==== shifrlash, deshifrlash, kalit generatsiyalash====

ERI hosil qilsih, maxfiylikni ta’minlash, kalitlar almashish uchun====

shifrlash, deshifrlash, kalitlar boshqarish uchun

++++

Assimmetrik kriptotizimlarda axborotni shifrlashda va deshifrlash uchun nechta kalit ishlatiladi?====

#Ikkita kalit==== Bitta kalit==== Uchta kalit====

Foydalanuvchi identifikatori

++++

Asosan tarmoq, tizim va tashkilot haqidagi axborotni olish maqasadida amalga oshiriladigan tarmoq hujumini belgilang. ====

#Razvedka hujumlari==== Kirish hujumlari====

DOS hujumi==== Zararli hujumlar

++++

Atribute based access control ABAC usuli attributlari qaysilar? ==== #Foydalanuvchi attributlari====

Asosiy va qo‘shimcha atributlar ==== Tizim attributlari, server atributlari ==== Ichki va tashqi attributlar

++++

Autentifikatsiyaga ta'rif qaysi javobda keltirilgan? ====

#Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi====

Tizim meyoriy va g‘ayritabiiy hollarda rejalashtirilgandek o‘zini tutishligi holati==== Istalgan vaqtda dastur majmuasining mumkinligini kafolati====

Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi

++++

Avtorizatsiya qanday jarayon?====

#foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni====

axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo‘yicha solishtirib uni aniqlash jarayoni====

obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash. ====

foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni

++++

Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?

====

#Korporativ va umumfoydalanuvchi==== Regional, korporativ====

Lokal, global==== Shaharlararo, lokal, global

++++

Axborot paketlarini qachon ushlab qolish mumkin? ==== #Aloqa kanallari orqali uzatishda====

Xotira qurilmalarida saqlanayotganda==== Kompyuter ishga tushganda==== Ma’lumotlar nusxalanayotganda

++++

Axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi nima deb ataladi? ====

#Axborot resursi ==== Axborot xavfsizligi==== Ma'lumotlar bazasi====

Axborot tizimlari

++++

Axborot tizimiga ta’rif bering. ====

#Qo'yilgan maqsadga erishish yo'lida axborotlarni olish, qayta ishlash, va uzatish uchun usullar, vositalar va xodimlar jamlanmasi====

Material olamda axborot almashinuvining yuzaga kelishini ta’minlovchi axborot uzatuvchi, aloqa kanallari, qabul qilgich vositalar jamlanmasi====

Qo'yilgan maqsadga erishish yo'lida o'zaro birlashtirilgan va ayni vaqtda yagona deb qaraluvchi elementlar to'plami====

Ishlab chiqarish jarayonida insonlarning umumiy munosabatlarini ifodalovchi vositlar to'plami

++++

Axborot xavfsizligi siyoatining necha xil turi bor? ==== #3====

4====

5====

2

++++

Axborot xavfsizligi siyosati –bu …====

#tashkilot o‘z faoliyatida rioya qiladigan axborot xavfsizligi sohasidagi hujjatlangan qoidalar, muolajalar, amaliy usullar yoki amal qilinadigan prinsiplar majmui sanalib, u asosida tashkilotda axborot xavfsizligi ta’minlanadi====

mavjud tahdidni amalga oshirilgan ko‘rinishi bo‘lib, bunda kutilgan tahdid amalga oshiriladi====

mavjud bo‘lgan zaiflik natijasida bo‘lishi mumkin bo‘lgan hujum turi bo‘lib, ular asosan tizimni kamchiliklarini o‘rganish natijasida kelib chiqadi====

tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

++++

Axborot xavfsizligida axborotning bahosi qanday aniqlanadi? ====

#Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan====

Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhumligi bilan====

Axborotni noqonuniy foydalanishlardan o‘zgartirishlardan va yo‘q qilishlardan himoyalanganligi bilan====

Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bilan

++++

Axborot xavfsizligini ta'minlovchi choralarni ko‘rsating? ==== #1-huquqiy, 2-tashkiliy-ma'muriy, 3-dasturiy-texnik====

1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy==== 1-amaliy, 2-tashkiliy-ma'muriy, 3-huquqiy====

1-apparat, 2-texnikaviy, 3-huquqiy

++++

Axborotdan oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan? ==== #AQSH sog'liqni saqlash va insonlarga xizmat ko'rsatish vazirligi====

AQSH Mudofaa vazirligi====

O'zbekiston Axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi==== Rossiya kiberjinoyatlarga qarshu kurashish davlat qo'mitasi

++++

Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? ==== #USB fleshka, CD va DVD disklar====

Qattiq disklar va CDROM==== CD va DVD, kesh xotira==== Qattiq disklar va DVDROM

++++

Axborotni himoyalash uchun ... usullari qo‘llaniladi. ==== #kodlashtirish, kriptografiya, stegonografiya====

shifrlash va kriptografiya, maxsus yozilgan kod==== Stegonografiya, kriptografiya, orfografiya==== Kriptoanaliz, kodlashtirish, zahiralash

++++

Axborotning buzilishi yoki yo‘qotilishi xavfiga olib keluvchi himoyalanuvchi obyektga qarshi qilingan xarakatlar qanday nomlanadi? ====

#Tahdid==== Zaiflik==== Hujum==== Butunlik

++++

Axborotning eng kichik o‘lchov birligi nima? ==== #bit====

kilobayt==== bayt==== kilobit

++++

Axbоrоt tizimlari xavfsizligining auditi-bu…====

#Axborot tizimlarining himoyalanishining joriy holati, tizim haqida obyektiv ma’lumotlarni olish va baholash====

Ma`lumоtlarini tahlillash va chоra ko‘rishni tizim haqida subyektiv ma’lumotlarni olish va baholashni tahlil qiladi====

Ma`lumоtlarini tarqatish va boshqarish==== Axbоrоtni yig‘ish va korxona tarmog‘ini tahlillash

++++

TrueCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? ==== #AES, Serpent va Twofish ====

Serpent, RSA====

El-Gamal, Twofish ====

DES

++++

"Bag" atamasini nima ma'noni beradi?====

#Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo'lgan muammo==== Mualliflik huquqini buzilishi====

Dasturlardagi ortiqcha reklamalar==== Autentifikatsiya jarayonini buzish

++++

"Barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti".- Bular tarmoqning qaysi sathiga kiradi? ====

#Fizik sath (physical) ==== Tarmoq sathi====

Amaliy sath==== Tadbiqiy sath

++++

Bell-LaPadula (BLP) modeli -bu.. ====

#Bu hukumat va harbiy dasturlarda kirishni boshqarishni kuchaytirish uchun ishlatiladigan avtomatlashgan modeli====

Axborlarni nazoratlovchi model====

Foydalanuvchilarni ro'yxatga olish , nazoratlash va tahlil qiluvchi model==== Tarmoq boshqarish va tahlil qiluvchi model

++++

Bell-LaPadula axborot xavfsizligida axborotni qaysi parametrini ta'minlash uchun xizmat qiladi?

====

#Konfidentsiallikni==== Yaxlitlikni==== Maxfiylikni==== O'zgarmaslikni

++++

Biba modeli obyektni qaysi xusuiyatiga e'tibor qaratilgan? ==== #Yaxlitligi====

Maxfiyligi==== Xavfsizligi==== Konfidentsialligi

++++

BiBa modeli qaysi modelning keygaytirilgan varianti hisoblanadi? ==== #Bell-Lapadula modeli====

RBAC==== MAC==== ABAC

++++

Biometrik parametrlarda xavfsizlik tomonidan kamchiligi nimadan iborat? ==== #ID ni almashtirish murakkabligi====

Foydalanish davrida maxfiylik kamayib boradi==== Qalbakilashtirish oson====

Parol va PIN kod ishlatilmasligi

++++

Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang. ==== #Shaxsiy simsiz tarmoq ====

Lokal simsiz tarmoq ==== Regional simsiz tarmoq ==== Global simsiz tarmoq

++++

Botnet-nima? ====

#internet tarmog'idagi obro'sizlantirilgan kompyuterlar bo'lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi====

zararli dasturiy vosita bo'lib, biror mantiqiy shart qanoatlantirilgan vaqtda o'z harakatini amalga oshiradi====

zararli dasturiy kodlar bo'lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o'tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo'lish. ====

ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

++++

…-bu so‘z ingliz tilidan olingan bo‘lib- yorib tashlash, chopish, buzish degan ma’nolarni anglatadi. Ular xaddan ziyod malakali va bilimli, axborot texnologiyalarini puxta biluvchi insondir.-Yuqoridagi fikr kim to‘g‘risida ta’rif berilgan? ====

#Xaker==== Dasturchi==== Tarmoq josusi==== Administrator

++++

Bulutli texnologiyalarda PaaS nimani ifodalaydi?==== #Platforma sifatida====

Servis sifatida==== Ma'lumot sifatida==== Prizentatsiya sifatida

|  |  |  |
| --- | --- | --- |
| 1 | Xavfsizlikning asosiy yo’nalishlarini sanab o’ting. | Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik |
| 2 | Axborot xavfsizligining asosiy maqsadlaridan biri- bu… | Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish |
| 3 | Konfidentsiallikga to’g’ri ta`rif keltiring. | axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; |
| 4 | Yaxlitlikni buzilishi bu - … | Soxtalashtirish va o’zgartirish |
| 5 | ... axborotni himoyalash tizimi deyiladi. | Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning  kompleksi |
| 6 | Kompyuter virusi nima? | maxsus yozilgan va zararli dastur |
| 7 | Axborotni himoyalash uchun ... usullari qo’llaniladi. | kodlashtirish, kriptografiya, stegonografiya |
| 8 | Stenografiya mahnosi... | sirli yozuv |
| 9 | Kriptologiya yo’nalishlari nechta? | 2 |
| 10 | Kriptografiyaning asosiy maqsadi... | maxfiylik, yaxlitlilikni ta`minlash |
| 11 | SMTP - Simple Mail Transfer protokol nima? | elektron pochta protokoli |
| 12 | SKIP protokoli... | Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi |
| 13 | Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar… | uzilish, tutib qolish, o’zgartirish, soxtalashtirish |
| 14 | ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. | konfidentsiallik |

|  |  |  |
| --- | --- | --- |
| 15 | Foydalanish huquqini cheklovchi matritsa modeli bu... | Bella La-Padulla modeli |
| 16 | Kommunikatsion qism tizimlarida xavfsizlikni ta`minlanishida necha xil shifrlash ishlatiladi? | 2 |
| 17 | Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? | TCP/IP, X.25 protokollar |
| 18 | Himoya tizimi kompleksligiga nimalar orqali erishiladi? | Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali |
| 19 | Kalit – bu … | Matnni shifrlash va shifrini ochish uchun kerakli axborot |
| 20 | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | simmetrik kriptotizimlar |
| 21 | Autentifikatsiya nima? | Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi |
| 22 | Identifikatsiya bu- … | Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni |
| 23 | O’rin almashtirish shifri bu - … | Murakkab bo’lmagan kriptografik akslantirish |
| 24 | Simmetrik kalitli shifrlash tizimi necha turga bo’linadi. | 2 turga |
| 25 | Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular … | hosil qilish, yig’ish, taqsimlash |
| 26 | Kriptologiya - | axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi |
| 27 | Kriptografiyada alifbo – | axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam |
| 28 | Simmetrik kriptotizimlarda ... jumlani davom ettiring | shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi |
| 29 | Kriptobardoshlilik deb … | kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
| 30 | Elektron raqamli imzo deb – | xabar muallifi va tarkibini aniqlash maqsadida  shifrmatnga qo’shilgan qo’shimcha |

|  |  |  |
| --- | --- | --- |
| 31 | Kriptografiya – | axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq  qiladi |
| 32 | Kriptografiyada matn – | alifbo elementlarining tartiblangan to’plami |
| 33 | Kriptoanaliz – | kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
| 34 | Shifrlash – | akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi |
| 35 | Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi? | Tez, aniq va maxfiyligiga |
| 36 | Faol hujum turi deb… | Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon |
| 37 | Blokli shifrlash- | shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish |
| 38 | Simmetrik kriptotizmning uzluksiz tizimida … | ochiq matnning har bir harfi va simvoli alohida shifrlanadi |
| 39 | Kripto tizimga qo’yiladigan umumiy talablardan biri | shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak |
| 40 | Quyidagi tengliklardan qaysilari shifrlash va deshifrlashni ifodalaydi? | Ek1(T)=T, Dk2(T1)=T |
| 41 | Berilgan ta`riflardan qaysi biri assimmetrik tizimlarga xos? | Assimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi |
| 42 | Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang | Vijiner matritsasi, Sezar usuli |
| 43 | Akslantirish tushunchasi deb nimaga aytiladi? | 1-to’plamli elementlariga 2- to’plam elementalriga mos bo’lishiga |
| 44 | Simmetrik guruh deb nimaga aytiladi? | O’rin almashtirish va joylashtirish |
| 45 | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | simmetrik kriptositemalar |

|  |  |  |
| --- | --- | --- |
| 46 | Xavfli viruslar bu - … | kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
| 47 | Mantiqiy bomba – bu … | Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
| 48 | Elektron raqamli imzo tizimi qanday muolajani amalga oshiradi? | raqamli imzoni shakllantirish va tekshirish muolajasi |
| 49 | Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? | Simmetrik va assimetrik |
| 50 | Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin? | Korporativ va umumfoydalanuvchi |
| 51 | Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo’linadi? | Sust va faol |
| 52 | Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? | SMTP, POP yoki IMAR |
| 53 | Axborot resursi – bu? | axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi |
| 54 | Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu? | login |
| 55 | Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu? | parol |
| 56 | Identifikatsiya jarayoni qanday jarayon? | axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash  jarayoni |
| 57 | Autentifikatsiya jarayoni qanday jarayon? | ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash |

|  |  |  |
| --- | --- | --- |
| 58 | Avtorizatsiya jarayoni qanday jarayon? | foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni |
| 59 | Ro’yxatdan o’tish bu? | foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni |
| 60 | Axborot qanday sifatlarga ega bo’lishi kerak? | ishonchli, qimmatli va to’liq |
| 61 | Axborotning eng kichik o’lchov birligi nima? | bit |
| 62 | Elektronhujjatning rekvizitlari nechta qismdan iborat? | 4 |
| 63 | Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? | fleshka, CD va DVD disklar |
| 64 | Imzo bu nima ? | hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini  tasdiqlaydigan insonning fiziologik xususiyati. |
| 65 | Muhr bu nima? | hujjatning haqi-qiyligini va biror bir yuridik shaxsga tegishli ekanligi-ni tasdiqlovchi isbotdir. |
| 66 | DSA – nima | Raqamli imzo algoritmi |
| 67 | El Gamal algoritmi qanday algoritm | Shifrlash algoritmi va raqamli imzo algoritmi |
| 68 | Sezarning shifrlash sistemasining kamchiligi | Harflarning so’zlarda kelish chastotasini yashirmaydi |
| 69 | Axborot xavfsizligi va xavfsizlik san’ati haqidagi fan …. deyiladi? | Kriptografiya |
| 70 | Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu - | steganografiya |
| 71 | Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? | Deshifrlash |
| 72 | …… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. | Kiberxavfsizlik |
| 73 | Risk | Potensial foyda yoki zarar |
| 74 | Kiberxavfsizlik nechta bilim soxasini o‘z ichiga oladi. | 8 |
| 75 | “Ma’lumotlar xavfsizligi” bilim sohasi...... | ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi. |

|  |  |  |
| --- | --- | --- |
| 76 | “Dasturiy ta’minotlar xavfsizligi” bilim sohasi..... | foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi. |
| 77 | “Tashkil etuvchilar xavfsizligi” ..... | katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va  texnik xizmat ko‘rsatishga e’tibor qaratadi. |
| 78 | “Aloqa xavfsizligi” bilim sohasi...... | tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni  birlashtiradi. |
| 79 | “Tizim xavfsizligi” bilim sohasi…… | tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi. |
| 80 | “Inson xavfsizligi” bilim sohasi…. | kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi. |
| 81 | “Tashkilot xavfsizligi” bilim sohasi …. | tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini |
| 82 | “Jamoat xavfsizligi” bilim sohasi ….. | u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi. |
| 83 | Tahdid nima? tizim yoki | Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
| 84 | Kodlash nima? | Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni  boshqa formatga o‘zgartirishdir |

|  |  |  |
| --- | --- | --- |
| 85 | Shifrlash nima? | Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi |
| 86 | Bir martalik bloknotda Qanday kalitlardan foydalaniladi? | Ochiq kalitdan |
| 87 | Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing. | 23 |
| 88 | Agar RSA algotirmida n ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi. | M = Cd mod n; |
| 89 | O’nlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq tizi miga o’tkazing. 65 | 100001 |
| 90 | Quyidagi modulli ifodani qiymatini toping. (125\*45)mod10. | 5 |
| 91 | Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256. | 244 |
| 92 | Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi. | C = Me mod n; -tog’ri javob |
| 93 | Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi | Kriptologiya. |
| 94 | Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi | {*d, n*} – yopiq, {*e, n*} – ochiq; |
| 95 | Zamonaviy kriptografiya qanday bo’limlardan iborat? | Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish |
| 96 | 1. Kriptografik usullardan foydalanishning asosiy yo’nalishlari nimalardan iborat? | Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarni haqiqiyligini aniqlash, tashuvchilarda axborotlarni shifrlangan ko’rinishda saqlash (masalan, hujjatlarni, ma’lumotlar bazasini) |
| 97 | Shifr nima? | Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm |
| 98 | Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? | Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi |

|  |  |  |
| --- | --- | --- |
| 99 | Oqimli shifrlashning mohiyati nimada? | Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur, Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi |
| 100 | Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating. | uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim, |
| 101 | Kriptotizim quyidagi komponentlardan iborat: | ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, Ek : M ® C (shifrlash uchun) va Dk: C®M (deshifrlash uchun)  funktsiyalar |
| 102 | Serpent, Square, Twofish, RC6 , AES algoritmlari qaysi turiga mansub? | simmetrik blokli algoritmlar |
| 103 | DES algoritmiga muqobil bo’lgan algoritmni ko’rsating. | Uch karrali DES, IDEA, Rijndael |
| 104 | DES algoritmining asosiy muammosi nimada? | kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas |
| 105 | Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? | shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun |
| 106 | 12+22 mod 32 ? | 2 |
| 107 | 2+5 mod32 ? | 7 |
| 108 | Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi. | ochiq kalitlar |
| 109 | 12+11 mod 16 ? | 7 |

|  |  |  |
| --- | --- | --- |
| 110 | RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo’llab quvvatlaydi. | 128 bitli, 192 bitli, 256 bitli |
| 111 | Xesh-funktsiyani natijasi … | uzunlikdagi xabar |
| 112 | RSA algoritmi qanday jarayonlardan tashkil topgan | Kalitni generatsiyalash; Shifrlash; Deshifrlash. |
| 113 | RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida necha bit bo‘lishi talab etiladi. | 2048 |
| 114 | Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi | Xesh funksiyalar |
| 115 | To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub | Xalqa |
| 116 | Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo’llamasligi mumkin | to’liq bog’lanishli |
| 117 | Kompyuterning tashqi interfeysi deganda nima tushuniladi | kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari  to’plamlari |
| 118 | Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi | Yulduz |
| 119 | Ethernet kontsentratori qanday vazifani bajaradi | kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib  beradi |
| 120 | OSI modelida nechta sath mavjud | 7 |
| 121 | OSI modelining to’rtinchi sathi qanday nomlanadi | Transport sathi |
| 122 | OSI modelining beshinchi sathi qanday nomlanadi | Seanslar sathi |
| 123 | OSI modelining birinchi sathi qanday nomlanadi | Fizik sath |
| 124 | OSI modelining ikkinchi sathi qanday nomlanadi | Kanal sathi |
| 125 | OSI modelining uchinchi sathi qanday nomlanadi | Tarmoq sathi |
| 126 | OSI modelining oltinchi sathi qanday nomlanadi | Taqdimlash sathi |
| 127 | OSI modelining ettinchi sathi qanday nomlanadi | Amaliy sath |
| 128 | OSI modelining qaysi sathlari tarmoqqa bog’liq sathlar hisoblanadi | fizik, kanal va tarmoq sathlari |
| 129 | OSI modelining tarmoq sathi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi | Marshrutizator |
| 130 | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi | Fizik sath |
| 131 | Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi sathi bajaradi | Tarmoq sathi |
| 132 | Keltirilgan protokollarning qaysilari tarmoq sathi protokollariga mansub | IP, IPX |

|  |  |  |
| --- | --- | --- |
| 133 | Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub | TCP,UDP |
| 134 | OSI modelining fizik sathi qanday funktsiyalarni bajaradi | Elektr signallarini uzatish va qabul qilish |
| 135 | OSI modeliningamaliy sathi qanday funktsiyalarni bajaradi | Klient dasturlari bilan o’zaro muloqotda bo’lish |
| 136 | Keltirilgan protokollarning qaysilari kanal sathi protokollariga mansub | Ethernet, FDDI |
| 137 | Keltirilgan protokollarning qaysilari taqdimlash sathi protokollariga mansub | SNMP, Telnet |
| 138 | Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni  bu... | Avtorizatsiya |
| 139 | Autentifikatsiya faktorlari nechta | 3 |
| 140 | Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima | Parol |
| 141 | Ko‘z pardasi, yuz tuzilishi, ovoz tembri. | Biometrik autentifikatsiya |
| 142 | barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi. | Fizik satx |
| 143 | Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi | 2 |
| 144 | Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi. | Foydalanishni boshqarish |
| 145 | Foydalanishni boshqarish –bu... | sub’ektni sub’ektga ishlash qobilyatini aniqlashdir. |
| 146 | Foydalanishna boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi, | Sub’ekt |
| 147 | Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ? | Ob’ekt |
| 148 | Foydalanishna boshqarishning nechta usuli  mavjud? | 4 |
| 149 | Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy ob’ektlarni himoyalash uchun qo‘llaniladi | DAC |
| 150 | Foydalanishni boshqarishning qaysi modelida ob’ekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi | DAC |
| 151 | Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi. | MAC |

|  |  |  |
| --- | --- | --- |
| 152 | Foydalanishni boshqarishning mandatli modelida Ob’ektning xavfsizlik darajasi nimaga bog‘liq.. | Tashkilotda ob’ektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi |
| 153 | MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi | xavfsizlik siyosati ma’muri |
| 154 | Agar sub’ektning xavfsizlik darajasida ob’ektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi | O‘qish |
| 155 | Agar sub’ektning xavfsizlik darajasi ob’ektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi. | Yozish |
| 156 | Foydalanishni boshqarishning qaysi modelida har bir ob’ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun ob’ektlardan foydalanish ruxsati ko‘rsatiladi? | RBAC |
| 157 | Rol tushunchasiga ta’rif bering. | Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin |
| 158 | Foydalanishni boshqarishning qaysi usuli - ob’ektlar va sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. | ABAC |
| 159 | XACML foydalanishni boshqarishni qaysi usulining standarti? | ABAC |
| 160 | Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan? | barchasi |
| 161 | Axborotning kriptografik himoya vositalari necha turda? | 3 |
| 162 | Dasturiy shifrlash vositalari necha turga bo‘linadi | 4 |
| 163 | Diskni shifrlash nima uchun amalga oshiriladi? | Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi |
| 164 | Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi? | 4 |
| 165 | Kompyuter tarmoqlari bu – | Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi |

|  |  |  |
| --- | --- | --- |
| 166 | Tarmoq modeli –bu.. ikki | Hisoblash tizimlariorasidagi aloqani ularning ichki tuzilmaviy vatexnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir to‘plami |
| 167 | OSI modelida nechta tarmoq sathi bor | 7 |
| 168 | OSI modeli 7 stahi bu | Ilova |
| 169 | OSI modeli 1 stahi bu | Fizik |
| 170 | OSI modeli 2 stahi bu | Kanal |
| 171 | TCP/IP modelida nechta satx mavjud | 4 |
| 172 | Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi. | Shaxsiy tarmoq |
| 173 | Tarmoq kartasi bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
| 174 | Switch bu... | Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi |
| 175 | Hab bu... | ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun  xizmat qiladi. |
| 176 | Tarmoq repiteri bu... | Signalni tiklash yoki qaytarish uchun foydalaniladi. |
| 177 | Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi. | DNS tizimlari |
| 178 | ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. | TCP |
| 179 | …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi. | UDP |
| 180 | Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi. | IP |
| 181 | Tarmoq taxdidlari necha turga bo‘linadi | 4 |
| 182 | Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; | Razvedka hujumlari |
| 183 | Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi | Kirish hujumlari |

|  |  |  |
| --- | --- | --- |
| 184 | Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi; | Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari |
| 185 | Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi; | Zararli hujumlar |
| 186 | Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? | Imzo qo‘yish va imzoni tekshirishdan |
| 187 | Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? | Imzo muallifining ochiq *kaliti yordamida* |
| 188 | Tarmoq modeli-bu... | Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir |
| 189 | OSI modeli nechta sathga ajraladi? | 7 |
| 190 | Fizik sathning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
| 191 | Ilova sathning vazifasi nimadan iborat | Ilovalarni tarmoqqa ulanish jarayoni |
| 192 | Kanal sathning vazifasi nimadan iborat | Fizik manzillash |
| 193 | Tarmoq sathning vazifasi nimadan iborat | Yo‘lni aniqlash va mantiqiy manzillash |
| 194 | TCP/IP modeli nechta sathdan iborat | 4 |
| 195 | Quyidagilarninf qaysi biri Kanal sathi protokollari | Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35. |
| 196 | Quyidagilarninf qaysi biri tarmoq sathi protokollari | . IP, ICMP, ARP, RARP |
| 197 | Quyidagilarninf qaysi biri transport sathi protokollari | TCP, UDP, RTP |
| 198 | Quyidagilarninf qaysi biri ilova sathi protokollari | HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP va hak |
| 199 | TCP/IP modelining kanal sathiga OSI modelining qaysi sathlari mos keladi | Kanal, Fizik |
| 200 | TCP/IP modelining tarmoq sathiga OSI modelining qaysi sathlari mos keladi | Tarmoq |
| 201 | TCP/IP modelining transport sathiga OSI modelining qaysi sathlari mos keladi | Tramsport |
| 202 | TCP/IP modelining ilova sathiga OSI modelining qaysi sathlari mos keladi | Ilova, taqdimot, seans |
| 203 | Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |

|  |  |  |
| --- | --- | --- |
| 204 | Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang. | . Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir- biriga bog‘laydi. |
| 205 | Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang. | Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi |
| 206 | Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang. | Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini  taqdim etadi |
| 207 | Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
| 208 | Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan | Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi |
| 209 | Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan | Yuboriluvchi va qabul qilinuvchi ma’lumot TOKYeN yordamida manziliga yetkaziladi |
| 210 | Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan | Tarmoqdagi barcha kompyuter va tugunlar bir-biri  bilan o‘zaro bog‘langan bo‘ladi |
| 211 | Tarmoq kartasi nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
| 212 | Repetir nima? | Odatda signalni tiklash yoki qaytarish uchun foydalaniladi |
| 213 | Hub nima? | Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun  xizmat qiladi |
| 214 | Switch nima? | Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga  uzatadi |

|  |  |  |
| --- | --- | --- |
| 215 | Router nima? | Qabul qilingan ma’lumotlarni tarmoq sathiga tegishli manzillarga ko‘ra (IP manzil) uzatadi |
| 216 | DNS tizimlari. | Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi |
| 217 | TCP bu- … | Transmission Control Protocol |
| 218 | UDP bu-… | User datagram protocol |
| 219 | Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang | Ichki, tashqi |
| 220 | Tarmoq xavfsizligining buzilishi natijasida biznes  faoliyatining buzilishi qanday oqibatlarga olib keladi | Biznes jarayonlarni to‘xtab qolishiga olib keladi |
| 221 | Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi | Hujum natijasida ishlab chiqarishi yo‘qolgan hollarda uni qayta tiklash ko‘p vaqt talab qiladi va bu vaqtda ishlab chiqarish to‘xtab qoladi |
| 222 | Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi | Konfidensial axborotni chiqib ketishi natijasida, tashkilot shaxsiy ma’lumotlarini yo‘qolishi mumkin |
| 223 | Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi | Tashkilot xodimlarining shaxsiy va ishga oid ma’ulmotlarini kutilmaganda oshkor bo‘lishi ushbu  xodimlarga bevosita ta’sir qiladi |
| 224 | Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli  bo‘lmasligi |
| 225 | Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi | tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi |
| 226 | Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. | Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi  choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi. |

|  |  |  |
| --- | --- | --- |
| 227 | Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi | Razvedka hujumlari |
| 228 | Ma’lumotlarni zaxira nusxalash bu – … | Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi |
| 229 | Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz | Zaxira nusxalash |
| 230 | Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
| 231 | Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi? | 5 |
| 232 | Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. | 4 |
| 233 | Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
| 234 | RAID texnologiyasining transkripsiyasi qanday. | Random Array of Independent Disks |
| 235 | RAID texnologiyasida nechta satx mavjud | 6 |
| 236 | OSI modelining birinchi sathi qanday nomlanadi | Fizik sath |
| 237 | OSI modelining ikkinchi sathi qanday nomlanadi | Kanal sathi |
| 238 | OSI modelining uchinchi sathi qanday nomlanadi | Tarmoq sathi |
| 239 | OSI modelining oltinchi sathi qanday nomlanadi | Taqdimlash sathi |
| 240 | OSI modelining ettinchi sathi qanday nomlanadi | Amaliy sath |
| 241 | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi | Fizik sath |
| 242 | Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub | TCP,UDP |
| 243 | OSI modelining fizik sathi qanday funktsiyalarni bajaradi | Elektr signallarini uzatish va qabul qilish |
| 244 | OSI modelining amaliy sathi qanday funktsiyalarni bajaradi | Klient dasturlari bilan o’zaro muloqotda bo’lish |
| 245 | 12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan sonlar soni nechta? | 8 ta |

|  |  |  |
| --- | --- | --- |
| 246 | Yevklid algoritmi qanday natijani beradi? | Sonning eng katta umumiy bo’luvchisini toppish |
| 247 | Qanday sonlar tub sonlar deb yuritiladi? | Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi. |
| 248 | To‘liq zaxiralash | To‘liq va o‘sib boruvchi usullarning mujassamlashgan ko‘rinishi bo‘lib, oxirgi zaxiralangan nusxadan boshlab bo‘lgan o‘zgarishlarni zaxira nusxalab boradi. • Amalga oshirish to‘liq zaxiralashga qaraganda tez amalga oshiriladi. • Qayta tiklash o‘sib boruvchi zaxiralashga qaraganda tez amalga oshiriladi. • Ma’lumotni saqlash uchun to‘liq zaxiralashga qaraganda kam joy talab etadi |

|  |  |  |
| --- | --- | --- |
| 249 | O‘sib boruvchi zaxiralash | Zaxiralangan ma’lumotga nisbatan o‘zgarish yuz berganda zaxirilash amalga oshiriladi. • Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usuli bo‘lishi mumkin (to‘liq saxiralashdan). • Saqlash uchun kam hajm va amalga oshirish jarayoni tez |
| 250 | Differensial zaxiralash | Ushbu zaxiralashda tarmoqga bog‘lanishamalga oshiriladi. • Iliq zaxiralashda, tizim yangilanishi davomiy yangilanishni qabul qilish uchun ulanadi |
| 251 | Ushbu jarayon ma’lumot qanday yo‘qolgani, ma’lumotni qayta tiklash dasturiy vositasi va ma’lumotni tiklash manzilini qayergaligiga bog‘liq bo‘ladi. Qaysi jarayon | Ma’lumotlarni qayta tiklash |
| 252 | Antivirus dasturlarini ko’rsating? | Drweb, Nod32, Kaspersky |
| 253 | Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi | wep, wpa, wpa2 |
| 254 | Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak? | ishonchli, qimmatli va to’liq |
| 255 | Axborotning eng kichik o’lchov birligi nima? | bit |
| 256 | Virtual xususiy tarmoq – bu? | VPN |
| 257 | Xavfli viruslar bu - … | kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
| 258 | Mantiqiy bomba – bu … | Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
| 259 | Rezident virus... | tezkor xotirada saqlanadi |
| 260 | DIR viruslari nimani zararlaydi? | FAT tarkibini zararlaydi |

|  |  |  |
| --- | --- | --- |
| 261 | .... kompyuter tarmoqlari bo’yicha tarqalib, komlg’yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi | «Chuvalchang» va replikatorli virus |
| 262 | Mutant virus... | shifrlash va deshifrlash algoritmlaridan iborat- to’g’ri javob |
| 263 | Fire Wall ning vazifasi... | tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi |
| 264 | Kompyuter virusi nima? | maxsus yozilgan va zararli dastur |
| 265 | Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating | disk, maxsus tashuvchi  qurilma va kompyuter tarmoqlari orqali |
| 266 | Troyan dasturlari bu... | virus dasturlar |
| 267 | Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? | 5 |
| 268 | Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud | detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar |
| 269 | Axborotni himoyalash uchun ... usullari qo’llaniladi. | kodlashtirish, kriptografiya, stegonografiya |
| 270 | Stenografiya mahnosi... | sirli yozuv |
| 271 | …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi | K.Shennon |
| 272 | Kriptologiya yo’nalishlari nechta? | 2 |
| 273 | Kriptografiyaning asosiy maqsadi... | maxfiylik, yaxlitlilikni ta`minlash |
| 274 | Zararli dasturiy vositalarni aniqlash turlari nechta | 3 |
| 275 | Signaiurana asoslangan | ...bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi  mumkin. |
| 276 | O‘zgarishni aniqlashga asoslangan | Zararli dasturlar biror joyda joylashishi sababli, agar tizimdagi biror joyga o‘zgarishni aniqlansa, u holda u zararlanishni ko‘rsatishi mumkin |
| 277 | Anomaliyaga asoslangan | Noodatiy yoki virusga o‘xshash yoki potensial zararli harakatlari yoki xususiyatlarni topishni maqsad qiladi |

|  |  |  |
| --- | --- | --- |
| 278 | Antiairuslar qanday usulda viruslarni aniqlaydi | Signaturaga asoslangan |
| 279 | Viruslar - | o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi |
| 280 | Rootkitlar- | ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi |
| 281 | Backdoorlar - | zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega  bo‘lish |
| 282 | Troyan otlari- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan  iborat bo‘ladi |
| 283 | Ransomware- | mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi |
| 284 | Resurslardan foydalanish usuliga ko’ra viruslar qanday turlarga bo’linadi | Virus parazit, Virus cherv |
| 285 | Zararlagan obyektlar turiga ko’ra | Dasturiy, yuklanuvchi, Makroviruslar, multiplatformali viruslar |
| 286 | Faollashish prinspiga ko’ra | Resident, Norezident |
| 287 | Dastur kodini tashkil qilish yondashuviga ko‘ra | Shifrlangan, shifrlanmagan, Polimorf |
| 288 | Shifrlanmagan viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud  bo‘lmaydi. |
| 289 | P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang | 840 |
| 290 | 256mod25=? | 6 |
| 291 | bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi. | Tizim |

|  |  |  |
| --- | --- | --- |
| 292 | Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima duyidadi | Xavfsizlik siyosati |
| 293 | RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday? | *p* va *q* –sonlarning ko‘paytmasini ifodalovchi sonning spektoriga teng; |
| 294 | DES algoritmi akslantirishlari raundlari soni qancha? | 16; |
| 295 | DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha? | CHap qism blok 32 bit, o‘ng qism blok 32 bit; |
| 296 | Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? | SHifrlash va deshifrlash jarayonlari uchun kalitlarni generatsiya qilish qoidalariga ko‘ra farqlanadi |
| 297 | 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta? | 18 ta |
| 298 | 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta? | 4 ta |
| 299 | Eyler funsiyasida 𝜙(1) qiymati nimaga teng? | 0 |
| 300 | Eyler funksiyasida 60 sonining qiymatini toping. | 59 |
| 301 | Eyler funksiyasi yordamida 1811 sonining qiymatini toping. | 1810 |
| 302 | 97 tub sonmi? | Tub |
| 303 | Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256. | 244 |
| 304 | Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220 | 44 |
| 305 | Quyidagi ifodani qiymatini toping. -17mod11 | 5 |
| 306 | 2 soniga 10 modul bo’yicha teskari sonni toping. | Ø |
| 307 | Tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta’minlash sohasidagi tadbirlar tavsiflanadigan yuqori darajadagi reja nima? | Kiberxavfsizlik siyosati |
| 308 | Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi? | tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi |
| 309 | Kiberxavfsizlikni ta’minlash masalalari bo’yicha xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang | SANS (System Administration Networking and Security) |

|  |  |  |
| --- | --- | --- |
| 310 | Korxonaning davomli muvaffaqiyat bilan faoliyat yuritishini ta’minlashga mo’ljallangan strukturalangan va o’zaro bog’langan harakatlar to’plami- … | Strategiya |
| 311 | Tahdidlarning muvaffaqiyatli amalga oshirilishiga imkon beruvchi har qanday omil – bu … | Zaiflik |
| 312 | ISO/IEC 27002:2005 – …. | Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari |
| 313 | O’zDStISO/IEC 27005:2013 – …. | Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish |
| 314 | Axborot xavfsizligi arxitekturasining nechta satxi bor? | 3 |
| 315 | Rahbariy hujjat. Ma’lumotlar uzatish tarmog’ida axborot xavfsizligini ta’minlash to’g’risida Nizom - Xujjat raqamini toping | RH 45-215:2009 |
| 316 | Davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta’minlash dasturini ishlab chiqish tartibi - Xujjat raqamini toping | RH 45-185:2011 |
| 317 | Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta’minlash darajasini aniqlash tartibi - Xujjat raqamini toping | RH 45-193:2007 |
| 318 | Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta’riflar - Xujjat raqamini toping | TSt 45-010:2010 |
| 319 | Quyidagilardan qaysi standart aloqa va axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta’riflarni belgilaydi? | TSt 45-010:2010 |
| 320 | Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni nima? | Identifikatsiya |
| 321 | Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima? | Autentifikatsiya |
| 322 | Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni – nima deyiladi? | Avtorizatsiya |
| 323 | Identifikatsiya nima? | Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish  jarayoni |

|  |  |  |
| --- | --- | --- |
| 324 | Autentifikatsiya nima? | Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni |
| 325 | Avtorizatsiya nima? | Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni |
| 326 | ... - Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o’tishni ta’minlovchi biror axborot | Parol |
| 327 | Smart karta o’lchamidagi, kichik xajmdagi xotira va xisoblash imkoniyatiga ega bo’lgan, o’zida parol yoki kalitni saqlovchi qurilma nima deb ataladi? | Token, Smartkarta |
| 328 | Smarkarta nima asosida autentifikatsiyalaydi? | Something you have |
| 329 | Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o’zgarib turadigan parol nima deyiladi? | One-time password (OTP) |
| 330 | Foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish nima deb ataladi? | Ma’murlash |
| 331 | Amaldagi qonunchilikka mos ravishda texnik, dasturiy va dasturiy-texnik vositalar yordamida axborot xavfsizligining nokriptografik usullari bilan ta’minlashni inobatga oluvchi axborot himoyasi nima? | Axborotning texnik himoyasi |
| 332 | Nazorat hududi – bu ... | Qo’riqlanuvchi soha bo’lib, uning ichida kommunikatsiya qurilmalari hamda axborot tarmog’ining lokal tarkibiy qurilmalarini birlashtiruvchi barcha nuqtalar joylashadi |

|  |  |  |
| --- | --- | --- |
| 333 | Texnik himoya vositalari – bu ... | Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob’ektni himoyalashdir |
| 334 | Bu axborotni tutib olish qurilmasi bo’lib, ularda uzatuvchi qurilma sifatida kontaktli mikrofonlardan foydalaniladi | Stetoskoplar |
| 335 | Xesh funktsiya to’g’ri ko’rsatilgan javobni  aniqlang. | MD5 |
| 336 | MD5, SHA1, Tiger xesh funktsiyalari uchun blok uzunligi necha baytga teng? | 64 bayt |
| 337 | Sub’ektni ob’ektga ishlash qobilyatini aniqlash – nima? | Foydalanishni boshqarish |
| 338 | Foydalanishni boshqarishda sub’ekt bu - .... | Inson, dastur, jarayon |
| 339 | Foydalanishni boshqarishning qaysi usuli tizimdagi shaxsiy ob’ektlarni ximoyalash uchun qo’llaniladi? | Discretionary access control DAC |
| 340 | Foydalanishni boshqarishning qaysi usulidan asosan operatsion tizimlarda qo’llaniladi? | Discretionary access control DAC |
| 341 | Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi? | Mandatory access control MAC |
| 342 | Foydalanishni boshqarishning qaysi usulida xavfsizlik markazlashgan tarzda xavfsizlik siyosati m’muri tomonidan amalga oshiriladi? | Mandatory access control MAC |
| 343 | Foydalanishni boshqarishning qaysi usulida xar bir foydalanuvchini foydalanish ruxsatini belgilash o’rniga rol uchun ob’ektlardan foydalanish ruxsatini ko’rsatish yetarli bo’ladi? | Role-based access control RBAC |
| 344 | Foydalanishni boshqarishning qaysi usulida sub’ekt va ob’ektlarga tegishli xuquqlarni ma’murlash oson kechadi? | Role-based access control RBAC |
| 345 | Firibgarlikni oldini olish uchun bir shaxs tomonidan ko’plab vazifalarni bajarishga ruxsat bermaslik zarur. Bu muammo foydalanishni boshqarishni qaysi usulida bartaraf etiladi? | Role-based access control RBAC |
| 346 | Ob’ekt va sub’ektlarning attributlari, ular bilan mumkin bo’lgan amallar va so’rovlarga mos keladigan muxit uchun qoidalarni taxlil qilish asosida foydalanishni boshqarish - .... | Attribute based access control ABAC |
| 347 | Attribute based access control ABAC usuli attributlari qaysilar? | Foydalanuvchi attributlari, Resurs attributlari, Ob’ekt va muxit attributlari |
| 348 | Foydalanishni boshqarishning qaysi usulida ruxsatlar va xarakatni kim bajarayotganligi to’g’risidagi xolatlar “agar, u xolda” buyrug’idan tashkil topgan qoidalarga asoslanadi? | Attribute based access control ABAC |

|  |  |  |
| --- | --- | --- |
| 349 | XASML standarti foydalanishni boshqarishning qaysi usulida qo’llaniladi? | Attribute based access control ABAC |
| 350 | XASML standartida qoida nima? | Maqsad, ta’sir, shart, majburiyat va maslaxatlar |
| 351 | XASML standartida maqsad nima? | Sub’ekt ob’ekt ustida nima xarakat qilishi |
| 352 | Lampsonning foydalanishni boshqarish matritsasi nimalardan tashkil topgan? | Imtiyozlar ro’yxati |
| 353 | Access control list va Capability list bu nimaning asosiy elementi xisoblanadi? | Lampson matritsasining |
| 354 | Lampson matritsasining satrlarida nima  ifodalanadi? | Sub’ektlar |
| 355 | Foydalanishni boshqarishning mantiqiy vositalari infratuzilma va uning ichidagi tizimlarda ... uchun foydalaniladi. | Mandat, Tasdiqlash, Avtorizatsiya |
| 356 | SHaxsiy simsiz tarmoq standartini aniqlang. | Bluetooth, IEEE 802.15,  IRDA |
| 357 | Lokal simsiz tarmoq standartini aniqlang. | IEEE 802.11, Wi-Fi,  HiperLAN |
| 358 | Regional simsiz tarmoq standartini aniqlang. | IEEE 802.16, WiMAX |
| 359 | Global simsiz tarmoq standartini aniqlang. | CDPD, 2G, 2.5G, 3G, 4G, 5G |
| 360 | Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang. | SHaxsiy simsiz tarmoq |
| 361 | IEEE 802.11, Wi-Fi, HiperLAN standartida ishlovchi simsiz tarmoq turini aniqlang. | Lokal simsiz tarmoq |
| 362 | IEEE 802.16, WiMAX standartida ishlovchi simsiz tarmoq turini aniqlang. | Regional simsiz tarmoq |
| 363 | CDPD, 2G, 2.5G, 3G, 4G, 5G standartida ishlovchi simsiz tarmoq turini aniqlang. | Global simsiz tarmoq |
| 364 | Bluetooth qanday chastota oralig’ida ishlaydi? | 2.4-2.485 Ggts |
| 365 | Wi-Fi qanday chastota oralig’ida ishlaydi? | 2.4-5 Ggts |
| 366 | WiMax tarmog’ining tezligi qancha? | 1 Gbit/sekund |
| 367 | Quyidagilardan qaysi biri MITM xujumiga tegishli xatti-xarakat ximoblanadi? | Aloqa seansini konfidentsialligini va yaxlitligini buzish |
| 368 | WiMAX tarmoq arxitekturasi nechta tashkil etuvchidan iborat? | 5 |
| 369 | WiMAX tarmoq arxitekturasi qaysi tashkil etuvchidan iborat? | Base station, Subscriber station, Mobile station, Relay station, Operator network |
| 370 | GSM raqamli mobil telefonlarining nechanchi avlodi uchun ishlab chiqilgan protokol? | Ikkinchi avlodi |
| 371 | GSM standarti qaysi tashkilot tomonidan ishlab chiqilgan? | European telecommunications standards institute |

|  |  |  |
| --- | --- | --- |
| 372 | .... – o’zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma’lumoti va xavfsizlik algoritmlarini saqlaydi. | Sim karta |
| 373 | Rutoken S qurilmasining og’irligi qancha? | 6.3 gramm |
| 374 | True Crypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES, Serpent, Twofish |
| 375 | Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidentsialligini aniqlash qaysi dasturiy shifrlash vositalarining vazifasi? | Disc encryption software |
| 376 | BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES, Serpent, Twofish |
| 377 | AxCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES-256 |
| 378 | Qog’oz ko’rinishidagi axborotlarni yo’q qilish qurilmasining nomini kiriting. | Shreder |
| 379 | Ma’lumotlarni bloklarga bo’lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya? | RAID 0 |
| 380 | Qaysi texnologiyada ma’lumotni ko’plab nusxalari bir vaqtda bir necha disklarga yoziladi? | RAID 1 |
| 381 | Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi? | RAID 3 |
| 382 | Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi? | RAID 5 |
| 383 | Disk zararlanganda “qaynoq almashtirish” yordamida uni almashtirish mumkin. Bu xususiyat qaysi texnologiyaga tegishli? | RAID 50 |
| 384 | Zaxiralashning qanday turlari mavjud? | To’liq, o’sib boruvchi, differentsial |
| 385 | IOS, Android, USB xotiralardan ma’lumotlarni tiklash uchun qaysi dasturdan foydalaniladi? | EASEUS Data recovery wizard |
| 386 | Foydalanuvchi ma’lumotlarini qo’lga kirituvchi va uni xujumchiga yuboruvchi dasturiy kod nima? | Spyware |
| 387 | Operatsion tizim tomonidan aniqlanmasligi uchun ma’lum xarakatlarni yashirish nima deyiladi? | Rootkits |
| 388 | Qurbon kompyuterda mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo’yib to’lov amalga oshirishni talab qiladi. Bu qaysi zararli dastur? | Ransomware |
| 389 | Quyidagilardan o’zidan ko’payishi yo’q bo’lganlarini belgilang. | Mantiqiy bomba, Troyan oti, Backdoors |
| 390 | Viruslar resurslardan foydalanish usuliga ko’ra qanday turlarga bo’linadi? | Virus parazitlar, virus chervlar |
| 391 | Viruslar zararlangan ob’ektlar turiga ko’ra qanday turlarga bo’linadi? | Dasturiy, yuklanuvchi, makroviruslar, ko’p  platformali |

|  |  |  |
| --- | --- | --- |
| 392 | Viruslar faollashish printsipiga ko’ra qanday turlarga bo’linadi? | Rezident, norezident |
| 393 | Viruslar dastur kodini tashkil qilish yondoshuviga ko’ra qanday turlarga bo’linadi? | SHifrlangan, shifrlanmagan, polimorf |
| 394 | Dastlabki virus nechanchi yilda yaratilgan? | 1988 |
| 395 | ILOVEYOU virusi keltirgan zarar qancha? | 10 mlrd. Dollar |
| 396 | CodeRed virusi keltirgan zarar qancha? | 2 mlrd. Dollar |
| 397 | Melissa virusi keltirgan zarar qancha? | 80 million dollar |
| 398 | NetSky virusi keltirgan zarar qancha? | 18 mlrd. Dollar |
| 399 | MyDoom virusi keltirgan zarar qancha? | 38 mlrd. Dollar |
| 400 | Risk monitoring ….. ni paydo bo’lish imkoniyatini aniqlaydi. | Yangi risklar |
| 401 | ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi. | Risk monitoring |
| 402 | Axborot xavfsizligi siyoatining necha hil turi bor? | 3 |
| 403 | Internetdan foydalanish siyosatining nechta turi mavjud? | 4 |
| 404 | Nomuntazam siyosat (Promiscuous Policy) nima? | Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi |
| 405 | Paranoid siyosati (Paranoid Policy) – bu …. | Hamma narsa ta’qiqlanadi |
| 406 | Ruxsat berishga asoslangan siyosat (Permissive Policy) – bu … | Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi |
| 407 | Ehtiyotkorlik siyosati (Prudent Policy) – bu …. | Barcha hizmatlar blokirovka qilingandan so’ng bog’lanadi |
| 408 | Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi. Bu qaysi xavfsizlik siyosatiga hos? | Nomuntazam siyosat (Promiscuous Policy) |
| 409 | Barcha hizmatlar blokirovka qilingandan so’ng bog’lanadi. Bu qaysi xavfsizlik siyosatiga hos? | Ehtiyotkorlik siyosati (Prudent Policy) |
| 410 | Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi. Bu qaysi xavfsizlik siyosatiga hos? | Ruxsat berishga asoslangan siyosat (Permissive Policy) |
| 411 | Hamma narsa ta’qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos? | Paranoid siyosati (Paranoid Policy) |
| 412 | Tizim arxitekturasining turlari nechta? | 5 |
| 413 | Internet, havo hujumidan mudofaa, transport tizimlari qaysi tizim arxitekturasiga xos? | Hamkorlik tizimlari arxitekturasi |
| 414 | Cloud computing texnologiyasining nechta asosiy turi mavjud? | 3 |
| 415 | Raqamli soatlar qaysi texnologiyaga tegishli? | O’rnatilgan tizimlar (Embedde systems) |
|  |  |  |

Xato

Qaysi siyosat tizim resurslarini foydalanishda hech qanday cheklovlar qo‘ymaydi?

Paranoid siyosat Zаxirаlаshning qаndаy turlаri mаvjud?

Ichki, tаshqi

Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ... .

Hakker

Axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi nima deb ataladi?

Axborot tizimlari

Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?

RAID 0

Spam bilan kurashishning dasturiy uslubida nimalar ko‘zda tutiladi?

Elektron pochta qutisiga kelib tushadigan spamlar me’yoriy xujjatlar asosida cheklanadi va bloklanadi

Botnet-nima?

zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish.

Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi?

RAID 5

Zararli dasturlar qanday turlarga bo‘linadi? Tabiiy dasturlar va suniy dasturlar

Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o‘z ichiga oladi?

Davlat va nodavlat tashkilotlari me’yorlarni Ma’lumotlarni zaxira nusxalash bu – …

Ma'lumotlar xavfsizligini ta'minlash uchun qo‘llaniladigan shifrlash jarayoni Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...

Global tarmoqdan uzib qo‘yish Dаstlаbki virus nechаnchi yildа yarаtilgаn?

1988

System-Specific SecurityPolicies, SSSP-bu… Muammoga qaratilgan xavfsizlik siyosati

Enterprise Information Security Policies, EISP-bu… Tizimga qaratilgan xavfizlik siyosati

Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?

"To‘liq zaxiralash"

"To‘q sariq kitob"da xavfsizlik kriteriyalari qanday bo‘limlardan iborat?

O‘ta maxfiy, maxfiy

TO’G’RILARI:

OSI modelida nechta tarmoq satxi bor ? J: 7

OSI modelining birinchi satxi qanday nomlanadi J: Fizik satx

OSI modelining ikkinchi satxi qanday nomlanadi J: Kanal satxi

OSI modelining uchinchi satxi qanday nomlanadi J: Tarmoq satxi

OSI modelining oltinchi satxi qanday nomlanadi J: Taqdimlash satxi

OSI modelining yettinchi satxi qanday nomlanadi J: Amaliy satx

OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi J: fizik, kanal va tarmoq satxlari

OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi J: Marshrutizator

OSI modelining fizik satxi qanday funktsiyalarni bajaradi J: Elektr signallarini uzatish va qabul qilish

Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ? J: Obyekt

Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi? J: Subyekt

Simmetrik kriptotizimlarda ... jumlani davom ettiring

J: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.

J: 2 turga

Axborotning eng kichik o’lchov birligi nima? J: bit

Ko‘z pardasi, yuz tuzilishi, ovoz tembri-: bular autentifikatsiyaning qaysi faktoriga mos belgilar? J: Biometrik autentifikatsiya

Kriptografiyaning asosiy maqsadi... J: maxfiylik, yaxlitlilikni ta`minlash Ro’yxatdan o’tish bu?

foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni

Qanday xujumda zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi? J: Zararli hujumlar

Qanday xujumda hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi?

J: Kirish hujumlari

Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub J: Ethernet, FDDI

Xesh-:funktsiyani natijasi …

J: fiksirlangan uzunlikdagi xabar

Ethernet kontsentratori qanday vazifani bajaradi

J: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?

J: fleshka, CD va DVD disklar Faol hujum turi deb…

J: Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon

Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi.

J: MAC

Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo‘llaniladi

J: DAC

Foydalanishni boshqarishning qaysi modelida Obyekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi

J: DACfInternetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?

Foydalanishni boshqarishning qaysi usuli -: Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

J: ABAC

Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun Obyektlardan foydalanish ruxsati ko‘rsatiladi? J: RBAC

To’rtta bir-:biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub

J: Xalqa Yulduz To’liq bog’lanishli Yacheykali

Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi?

J: DNS tizimlari, Razvedka hujumlari

…… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. J: Kiberxavfsizlik

Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi? J: raqamli imzoni shakllantirish va tekshirish muolajasi Kriptologiya -:

J: axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?

J: Deshifrlash

Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.

J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik

[Autentifikatsiya faktorlari](http://moodle.fbtuit.uz/mod/url/view.php?id=19891) nechta J: 3

Kriptografiyada matn –

J: alifbo elementlarining tartiblangan to’plami Konfidentsiallikga to’g’ri ta`rif keltiring.

J: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-:ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu?

J: login Kriptoanaliz –

J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi Axborot qanday sifatlarga ega bo’lishi kerak?

J: ishonchli, qimmatli va to’liq Shifrlash –

J: akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?

J: simmetrik kriptosistemalar Foydalanishni boshqarish –bu...

J: Subyektni Obyektga ishlash qobilyatini aniqlashdir. Kompyuterning tashqi interfeysi deganda nima tushuniladi?

J: kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari

Kodlash nima?

J: Ma’lumotni osongina qaytarish uchun hammaga Tarmoq kartasi bu...

J: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

Elektron raqamli imzo deb –

J: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha Hab bu...

J: ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Switch bu...

J: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.

Axborot xavfsizligining asosiy maqsadlaridan biri-: bu…

J: Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish

Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-:ketligi (maxfiy so’z) – bu?

J: parol

Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?

J: SMTP, POP yoki IMAR

Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi? J: Tez, aniq va maxfiyligiga

Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.

J: Yozish

Qanday xujumda hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi?

J: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari Kalit – bu …

J: Matnni shifrlash va shifrini ochish uchun kerakli axborot

Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi J: Fizik satx

Blokli shifrlash-:

J: shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish Kriptobardoshlilik deb …

J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi

J: Xesh funksiyalar Kriptografiya –

J: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub

J: TCP,UDP

Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu -: J: steganografiya

Yaxlitlikni buzilishi bu -: …

J: Soxtalashtirish va o’zgartirish

Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?

J: barchasi

Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub J: Ethernet, FDDI

Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? J: Foydalanishni boshqarish

Tarmoq repiteri bu…

J: Signalni tiklash yoki qaytarish uchun foydalaniladi. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

J: Ochiq kalitli kriptotizimlarda bir-:biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi

J: O‘qish

MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi

J: xavfsizlik siyosati ma’muri

Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?

J: Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi

J: Tarmoq satxi

Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bog‘liq..

J: Tashkilotda Obyektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi

Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi J: {d, n} – yopiq, {e, n} – ochiq;

Diskni shifrlash nima uchun amalga oshiriladi?

J: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi

Tahdid nima?

J: Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. Risk

J: Potensial foyda yoki zarar

barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi?

J: Fizik satx

Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...

J: Avtorizatsiya

Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.

J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik

Kompyuter tarmoqlari bu –

J: Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?

J: raqamli imzoni shakllantirish va tekshirish muolajasi Kriptografiyada matn –

J: alifbo elementlarining tartiblangan to’plami

Autentifikatsiya jarayoni qanday jarayon?

J: obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash

Rol tushunchasiga ta’rif bering.

J: Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin

Avtorizatsiya jarayoni qanday jarayon?

J: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima

J: Parol

Elektron raqamli imzo deb –

J: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha TCP/IP modelida nechta satx mavjud

J: 4

Kriptoanaliz –

J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi?

J: Simmetrik va assimetrik Shifrlash nima?

J: Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi

Kriptografiyada alifbo –

J: axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam Kripto tizimga qo’yiladigan umumiy talablardan biri

J: shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak Simmetrik kriptotizmning uzluksiz tizimida …

J: ochiq matnning har bir harfi va simvoli alohida shifrlanadi Axborot resursi – bu?

J: axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi Stenografiya ma’nosi...

J: sirli yozuv

Identifikatsiya jarayoni qanday jarayon?

J: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni

Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.

J: Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

1. Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq? J:simmetrik kriptotizimlar
2. Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.

J:Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.

1. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?

J: parol

1. Rol tushunchasiga ta’rif bering.

Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin

1. Foydalanish huquqini cheklovchi matritsa modeli bu... J:Bella La-Padulla modeli
2. Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? J: Deshifrlash
3. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

J:Strukturalarni ruxsatsiz modifikatsiyalash

1. Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi?

J:Kriptobardoshlik

1. Foydalanishni boshqarish –bu...

J: Sub’ektni Ob’ektga ishlash qobilyatini aniqlashdir.

1. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? J: Yulduz
2. RSA algoritm qaysi yilda ishlab chiqilgan? J: 1977 yil
3. Elektron xujjatlarni yo‘q qilish usullari qaysilar? J:Shredirlash, magnitsizlantirish, yanchish
4. Kriptografiyada kalitning vazifasi nima?

J: Matnni shifrlash va shifrini ochish uchun kerakli axborot

1. WiMAX qanday simsiz tarmoq turiga kiradi? J: Regional
2. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…

J: login

1. Stenografiya ma’nosi qanday? J: sirli yozuv
2. Fire Wall ning vazifasi...

J: Tarmoqlar orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta’minlaydi

1. Yaxlitlikni buzilishi bu - … J: Soxtalashtirish va o‘zgartirish
   1. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko‘rsating?

DDoS (Distributed Denial of Service) hujum

* 1. Rezident virus…

tezkor xotirada saqlanadi

* 1. Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyoti fanda qanday nomladi?

AKT xavfsizlik siyosati

* 1. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang. Recuva, R.saver
  2. Zaiflik – bu…

tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

* 1. Axborot xavfsizligi timsollarini ko‘rsating. Alisa, Bob, Eva
  2. Kiberetika tushunchasi:

Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

* 1. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuni qachon kuchga kirgan?

1997 yil 24 aprel

* 1. DIR viruslari nimani zararlaydi? FAT tarkibini zararlaydi
  2. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

Detektorlar

* 1. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?

"Issiq zaxiralash"

* 1. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...

Tamoqlararo ekranlarning o‘rnatilishi

* 1. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan

* 1. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…

Kiberjinoyat deb ataladi

* 1. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud?

detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar

* 1. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?

Ruxsat berishga asoslangan siyosat

* 1. DIR viruslari nimani zararlaydi? FAT tarkibini zararlaydi
  2. Makroviruslar nimalarni zararlaydi?

Ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.

* 1. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang. HandyBakcup
  2. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.

"Sovuq saxiralash"

* 1. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.

Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

* 1. Polimorf viruslar tushunchasi to‘g‘ri ko‘rsating.

Viruslar turli ko‘rinishdagi shifrlangan viruslar bo‘lib, o‘zining ikkilik shaklini nusxadan-nusxaga o‘zgartirib boradi

* 1. Fishing (ing. Phishing – baliq ovlash) bu…

Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

|  |  |  |
| --- | --- | --- |
| 24. | Xavfsizlikning asosiy yo’nalishlarini sanab o’ting. | Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik,  Ekologik xavfsizlik |
| 25. | Axborot xavfsizligining asosiy maqsadlaridan  biri- bu… | Axborotlarni o’g’irlanishini, yo’qolishini,  soxtalashtirilishini oldini olish |
| 26. | Konfidentsiallikga to’g’ri ta`rif keltiring. | axborot inshonchliligi, tarqatilishi mumkin  emasligi, maxfiyligi kafolati; |
| 27. | Yaxlitlikni buzilishi bu - … | Soxtalashtirish va o’zgartirish |
| 28. | ... axborotni himoyalash tizimi deyiladi. | Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning  kompleksi |
| 29. | Kompyuter virusi nima? | maxsus yozilgan va zararli dastur |
| 30. | Axborotni himoyalash uchun ... usullari  qo’llaniladi. | kodlashtirish, kriptografiya, stegonografiya |
| 31. | Stenografiya mahnosi... | sirli yozuv |
| 32. | Kriptologiya yo’nalishlari nechta? | 2 |
| 33. | Kriptografiyaning asosiy maqsadi... | maxfiylik, yaxlitlilikni ta`minlash |
| 34. | SMTP - Simple Mail Transfer protokol nima? | elektron pochta protokoli |
| 35. | SKIP protokoli... | Internet protokollari uchun kriptokalitlarning  oddiy boshqaruvi |
| 36. | Kompyuter tarmog’ining asosiy komponentlariga  nisbatan xavf-xatarlar… | uzilish, tutib qolish, o’zgartirish,  soxtalashtirish |
| 37. | ...ma`lumotlar oqimini passiv hujumlardan  himoya qilishga xizmat qiladi. | konfidentsiallik |
| 38. | Foydalanish huquqini cheklovchi matritsa modeli  bu... | Bella La-Padulla modeli |
| 39. | Kommunikatsion qism tizimlarida xavfsizlikni  ta`minlanishida necha xil shifrlash ishlatiladi? | 2 |
| 40. | Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi  standartlar yordamida amalga oshiriladi? | TCP/IP, X.25 protokollar |
| 41. | Himoya tizimi kompleksligiga nimalar orqali erishiladi? | Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning  mavjudligi orqali |
| 42. | Kalit – bu … | Matnni shifrlash va shifrini ochish uchun  kerakli axborot |
| 43. | Qo’yish, o’rin almashtirish, gammalash  kriptografiyaning qaysi turiga bog’liq? | simmetrik kriptotizimlar |
| 44. | Autentifikatsiya nima? | Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish  muolajasi |
| 45. | Identifikatsiya bu- … | Foydalanuvchini uning identifikatori (nomi)  bo’yicha aniqlash jarayoni |
| 46. | O’rin almashtirish shifri bu - … | Murakkab bo’lmagan kriptografik  akslantirish |

|  |  |  |
| --- | --- | --- |
| 47. | Simmetrik kalitli shifrlash tizimi necha turga  bo’linadi. | 2 turga |
| 48. | Kalitlar boshqaruvi 3 ta elementga ega bo’lgan  axborot almashinish jarayonidir bular … | hosil qilish, yig’ish, taqsimlash |
| 49. | Kriptologiya - | axborotni qayta akslantirib himoyalash  muammosi bilan shug’ullanadi |
| 50. | Kriptografiyada alifbo – | axborot belgilarini kodlash uchun  foydalaniladigan chekli to’plam |
| 51. | Simmetrik kriptotizimlarda ... jumlani davom  ettiring | shifrlash va shifrni ochish uchun bitta va  aynan shu kalitdan foydalaniladi |
| 52. | Kriptobardoshlilik deb … | kalitlarni bilmasdan shifrni ochishga  bardoshlilikni aniqlovchi shifrlash tavsifi |
| 53. | Elektron raqamli imzo deb – | xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan  qo’shimcha |
| 54. | Kriptografiya – | axborotni qayta akslantirishning matematik  usullarini izlaydi va tadqiq qiladi |
| 55. | Kriptografiyada matn – | alifbo elementlarining tartiblangan to’plami |
| 56. | Kriptoanaliz – | kalitlarni bilmasdan shifrni ochishga  bardoshlilikni aniqlovchi shifrlash tavsifi |
| 57. | Shifrlash – | akslantirish jarayoni: ochiq matn deb  nomlanadigan matn shifrmatnga almashtiriladi |
| 58. | Kalit taqsimlashda ko’proq nimalarga e`tibor  beriladi? | Tez, aniq va maxfiyligiga |
| 59. | Faol hujum turi deb… | Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar  tayyorlash harakatlaridan iborat jarayon |
| 60. | Blokli shifrlash- | shifrlanadigan matn blokiga qo’llaniladigan  asosiy akslantirish |
| 61. | Simmetrik kriptotizmning uzluksiz tizimida … | ochiq matnning har bir harfi va simvoli  alohida shifrlanadi |
| 62. | Kripto tizimga qo’yiladigan umumiy talablardan  biri | shifr matn uzunligi ochiq matn uzunligiga  teng bo’lishi kerak |
| 63. | Quyidagi tengliklardan qaysilari shifrlash va  deshifrlashni ifodalaydi? | Ek1(T)=T, Dk2(T1)=T |
| 64. | Berilgan ta`riflardan qaysi biri assimmetrik tizimlarga xos? | Assimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa  deshifrlanadi |
| 65. | Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish  usulini belgilang | Vijiner matritsasi, Sezar usuli |
| 66. | Akslantirish tushunchasi deb nimaga aytiladi? | 1-to’plamli elementlariga 2-to’plam  elementalriga mos bo’lishiga |
| 67. | Simmetrik guruh deb nimaga aytiladi? | O’rin almashtirish va joylashtirish |
| 68. | Qo’yish, o’rin almashtirish, gammalash  kriptografiyaning qaysi turiga bog’liq? | simmetrik kriptositemalar |
| 69. | Xavfli viruslar bu - … | kompyuter ishlashida jiddiy nuqsonlarga  sabab bo’luvchi viruslar |

|  |  |  |
| --- | --- | --- |
| 70. | Mantiqiy bomba – bu … | Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning  alohida modullari |
| 71. | Elektron raqamli imzo tizimi qanday muolajani  amalga oshiradi? | raqamli imzoni shakllantirish va tekshirish  muolajasi |
| 72. | Shifrlashning kombinatsiyalangan usulida qanday  kriptotizimlarning kriptografik kalitlaridan foydalaniladi? | Simmetrik va assimetrik |
| 73. | Axborot himoyasi nuqtai nazaridan kompyuter  tarmoqlarini nechta turga ajratish mumkin? | Korporativ va umumfoydalanuvchi |
| 74. | Elektromagnit nurlanish va ta`sirlanishlardan  himoyalanish usullari nechta turga bo’linadi? | Sust va faol |
| 75. | Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan  foydalaniladi? | SMTP, POP yoki IMAR |
| 76. | Axborot resursi – bu? | axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar  bazasi |
| 77. | Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga  ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu? | login |
| 78. | Uning egasi haqiqiyligini aniqlash jarayonida  tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu? | parol |
| 79. | Identifikatsiya jarayoni qanday jarayon? | axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va  berilgan nom bo’yicha solishtirib uni aniqlash jarayoni |
| 80. | Autentifikatsiya jarayoni qanday jarayon? | ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini  tekshirish orqali aslligini aniqlash |
| 81. | Avtorizatsiya jarayoni qanday jarayon? | foydalanuvchining resursdan foydalanish  huquqlari va ruxsatlarini tekshirish jarayoni |
| 82. | Ro’yxatdan o’tish bu? | foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq  berish jarayoni |
| 83. | Axborot qanday sifatlarga ega bo’lishi kerak? | ishonchli, qimmatli va to’liq |
| 84. | Axborotning eng kichik o’lchov birligi nima? | bit |
| 85. | Elektronhujjatning rekvizitlari nechta qismdan  iborat? | 4 |
| 86. | Axborotlarni saqlovchi va tashuvchi vositalar  qaysilar? | fleshka, CD va DVD disklar |
| 87. | Imzo bu nima ? | hujjatning haqiqiyligini va yuborgan fizik  shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati. |
| 88. | Muhr bu nima? | hujjatning haqi-qiyligini va biror bir yuridik  shaxsga tegishli ekanligi-ni tasdiqlovchi isbotdir. |

|  |  |  |
| --- | --- | --- |
| 89. | DSA – nima | Raqamli imzo algoritmi |
| 90. | El Gamal algoritmi qanday algoritm | Shifrlash algoritmi va raqamli imzo algoritmi |
| 91. | Sezarning shifrlash sistemasining kamchiligi | Harflarning so’zlarda kelish chastotasini  yashirmaydi |
| 92. | Axborot xavfsizligi va xavfsizlik san’ati haqidagi  fan …. deyiladi? | Kriptografiya |
| 93. | Tekstni boshqa tekst ichida ma’nosini yashirib  keltirish bu - | steganografiya |
| 94. | Shifrtekstni ochiq tekstga akslantirish jarayoni  nima deb ataladi? | Deshifrlash |
| 95. | …… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya,  inson, axborot va jarayonni mujassamlashtirgan. | Kiberxavfsizlik |
| 96. | Risk | Potensial foyda yoki zarar |
| 97. | Kiberxavfsizlik nechta bilim soxasini o‘z ichiga  oladi. | 8 |
| 98. | “Ma’lumotlar xavfsizligi” bilim sohasi...... | ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad  qiladi. |
| 99. | “Dasturiy ta’minotlar xavfsizligi” bilim sohasi..... | foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy  ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi. |
| 100 | “Tashkil etuvchilar xavfsizligi” ..... | katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga  e’tibor qaratadi. |
| 101 | “Aloqa xavfsizligi” bilim sohasi...... | tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va  mantiqiy ulanishni birlashtiradi. |
| 102 | “Tizim xavfsizligi” bilim sohasi…… | tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim  xavfsizligining aspektlariga e’tibor qaratadi. |
| 103 | “Inson xavfsizligi” bilim sohasi…. | kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor  qaratadi. |
| 104 | “Tashkilot xavfsizligi” bilim sohasi …. | tashkilotni kiberxavfsizlik tahdidlaridan  himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini |
| 105 | “Jamoat xavfsizligi” bilim sohasi ….. | u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga  e’tibor qaratadi. |
| 106 | Tahdid nima? tizim yoki | Tashkilotga zarar yetkazishi mumkin bo‘lgan  istalmagan hodisa. |
| 107 | Kodlash nima? | Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga  o‘zgartirishdir |

|  |  |  |
| --- | --- | --- |
| 108 | Shifrlash nima? | Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta  o‘zgartirishi mumkin bo‘ladi |
| 109 | Bir martalik bloknotda Qanday kalitlardan  foydalaniladi? | Ochiq kalitdan |
| 110 | Ikkilik sanoq tizimida berilgan 10111 sonini  o’nlik sanoq tizimiga o’tkazing. | 23 |
| 111 | Agar RSA algotirmida n ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni  ifodalaydi. | M = Cd mod n; |
| 112 | O’nlik sanoq tizimida berilgan quyidagi sonlarni  ikkil sanoq tizi miga o’tkazing. 65 | 100001 |
| 113 | Quyidagi modulli ifodani qiymatini toping.  (125\*45)mod10. | 5 |
| 114 | Quyidagi modulli ifodani qiymatini toping (148 +  14432) mod 256. | 244 |
| 115 | Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni  ifodalaydi. | C = Me mod n; -tog’ri javob |
| 116 | Axborotni shifrni ochish (deshifrlash) bilan  qaysi fan shug’ullanadi | Kriptologiya. |
| 117 | Qaysi juftlik RSA algoritmining ochiq va yopiq  kalitlarini ifodalaydi | {*d, n*} – yopiq, {*e, n*} – ochiq; |
| 118 | Zamonaviy kriptografiya qanday bo’limlardan iborat? | Simmetrik kriptotizimlar; ochiq kalitli  kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish |
| 119 | 1. Kriptografik usullardan foydalanishning asosiy yo’nalishlari nimalardan iborat? | Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarni haqiqiyligini aniqlash, tashuvchilarda axborotlarni  shifrlangan ko’rinishda saqlash (masalan, hujjatlarni, ma’lumotlar bazasini) |
| 120 | Shifr nima? | Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan  krptografik algoritm |
| 121 | Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? | Ochiq kalitli kriptotizimlarda bir-biri bilan  matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi |
| 122 | Oqimli shifrlashning mohiyati nimada? | Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur, Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur, Oqimli shifrlash  algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi |
| 123 | Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating. | uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga  bog’liq bo’lishi lozim, |

|  |  |  |
| --- | --- | --- |
| 124 | Kriptotizim quyidagi komponentlardan iborat: | ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, Ek : M ® C (shifrlash uchun) va Dk: C®M (deshifrlash uchun)  funktsiyalar |
| 125 | Serpent, Square, Twofish, RC6 , AES algoritmlari  qaysi turiga mansub? | simmetrik blokli algoritmlar |
| 126 | DES algoritmiga muqobil bo’lgan algoritmni  ko’rsating. | Uch karrali DES, IDEA, Rijndael |
| 127 | DES algoritmining asosiy muammosi nimada? | kalit uzunligi 56 bit. Bugungu kunda ushbu  uzunlik algoritmning kriptobardoshliligi uchun yetarli emas |
| 128 | Asimmetrik kriptotizimlar qanday maqsadlarda  ishlatiladi? | shifrlash, deshifrlash, ERI yaratish va  tekshirish, kalitlar almashish uchun |
| 129 | 12+22 mod 32 ? | 2 |
| 130 | 2+5 mod32 ? | 7 |
| 131 | Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda  ishlatiladi. | ochiq kalitlar |
| 132 | 12+11 mod 16 ? | 7 |
| 133 | RIJNDAEL algoritmi qancha uzunligdagi  kalitlarni qo’llab quvvatlaydi. | 128 bitli, 192 bitli, 256 bitli |
| 134 | Xesh-funktsiyani natijasi … | uzunlikdagi xabar |
| 135 | RSA algoritmi qanday jarayonlardan tashkil  topgan | Kalitni generatsiyalash; Shifrlash;  Deshifrlash. |
| 136 | RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida necha bit  bo‘lishi talab etiladi. | 2048 |
| 137 | Ma’lumotlar butunligi qanday algritmlar orqali  amalga oshiriladi | Xesh funksiyalar |
| 138 | To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya  turiga mansub | Xalqa |
| 139 | Qaysi topologiya birgalikda foydalanilmaydigan  muhitni qo’llamasligi mumkin | to’liq bog’lanishli |
| 140 | Kompyuterning tashqi interfeysi deganda nima tushuniladi | kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish  qoidalari to’plamlari |
| 141 | Lokal tarmoqlarda keng tarqalgan topologiya turi  qaysi | Yulduz |
| 142 | Ethernet kontsentratori qanday vazifani bajaradi | kompyuterdan kelayotgan axborotni qolgan  barcha kompyuterga yo’naltirib beradi |
| 143 | OSI modelida nechta sath mavjud | 7 |
| 144 | OSI modelining to’rtinchi sathi qanday nomlanadi | Transport sathi |
| 145 | OSI modelining beshinchi sathi qanday  nomlanadi | Seanslar sathi |
| 146 | OSI modelining birinchi sathi qanday nomlanadi | Fizik sath |
| 147 | OSI modelining ikkinchi sathi qanday nomlanadi | Kanal sathi |
| 148 | OSI modelining uchinchi sathi qanday nomlanadi | Tarmoq sathi |
| 149 | OSI modelining oltinchi sathi qanday nomlanadi | Taqdimlash sathi |
| 150 | OSI modelining ettinchi sathi qanday nomlanadi | Amaliy sath |

|  |  |  |
| --- | --- | --- |
| 151 | OSI modelining qaysi sathlari tarmoqqa bog’liq  sathlar hisoblanadi | fizik, kanal va tarmoq sathlari |
| 152 | OSI modelining tarmoq sathi vazifalari keltirilgan  qurilmalarning qaysi birida bajariladi | Marshrutizator |
| 153 | Elektr signallarini qabul qilish va uzatish  vazifalarini OSI modelining qaysi sathi bajaradi | Fizik sath |
| 154 | Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi sathi  bajaradi | Tarmoq sathi |
| 155 | Keltirilgan protokollarning qaysilari tarmoq sathi  protokollariga mansub | IP, IPX |
| 156 | Keltirilgan protokollarning qaysilari transport  sathi protokollariga mansub | TCP,UDP |
| 157 | OSI modelining fizik sathi qanday funktsiyalarni  bajaradi | Elektr signallarini uzatish va qabul qilish |
| 158 | OSI modeliningamaliy sathi qanday funktsiyalarni  bajaradi | Klient dasturlari bilan o’zaro muloqotda  bo’lish |
| 159 | Keltirilgan protokollarning qaysilari kanal sathi  protokollariga mansub | Ethernet, FDDI |
| 160 | Keltirilgan protokollarning qaysilari taqdimlash  sathi protokollariga mansub | SNMP, Telnet |
| 161 | Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni  bu... | Avtorizatsiya |
| 162 | Autentifikatsiya faktorlari nechta | 3 |
| 163 | Faqat foydalanuvchiga ma’lum va biror tizimda  autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima | Parol |
| 164 | Ko‘z pardasi, yuz tuzilishi, ovoz tembri. | Biometrik autentifikatsiya |
| 165 | barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun  quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi. | Fizik satx |
| 166 | Fizik xavfsizlikda Yong‘inga qarshi tizimlar  necha turga bo‘linadi | 2 |
| 167 | Avtorizatsiya tushunchasi odatda qaysi tushuncha  bilan sinonim sifatida ham foydalanadi. | Foydalanishni boshqarish |
| 168 | Foydalanishni boshqarish –bu... | sub’ektni sub’ektga ishlash qobilyatini  aniqlashdir. |
| 169 | Foydalanishna boshqarishda inson, dastur, jarayon  va xokazolar nima vazifani bajaradi, | Sub’ekt |
| 170 | Foydalanishna boshqarishda ma’lumot , resurs,  jarayon nima vazifani bajaradi ? | Ob’ekt |
| 171 | Foydalanishna boshqarishning nechta usuli  mavjud? | 4 |
| 172 | Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy ob’ektlarni himoyalash uchun  qo‘llaniladi | DAC |

|  |  |  |
| --- | --- | --- |
| 173 | Foydalanishni boshqarishning qaysi modelida ob’ekt egasining o‘zi undan foydalanish huquqini  va kirish turini o‘zi belgilaydi | DAC |
| 174 | Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni  klassifikatsiyalashga asosan boshqariladi. | MAC |
| 175 | Foydalanishni boshqarishning mandatli modelida Ob’ektning xavfsizlik darajasi nimaga bog‘liq.. | Tashkilotda ob’ektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan  zarar miqdori bilan xarakterlanadi |
| 176 | MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan  amalga oshiriladi | xavfsizlik siyosati ma’muri |
| 177 | Agar sub’ektning xavfsizlik darajasida ob’ektning  xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi | O‘qish |
| 178 | Agar sub’ektning xavfsizlik darajasi ob’ektning xavfsizlik darajasida bo‘lsa, u holda qanday  amalga ruxsat beriladi. | Yozish |
| 179 | Foydalanishni boshqarishning qaysi modelida har bir ob’ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun  ob’ektlardan foydalanish ruxsati ko‘rsatiladi? | RBAC |
| 180 | Rol tushunchasiga ta’rif bering. | Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi  mumkin |
| 181 | Foydalanishni boshqarishning qaysi usuli - ob’ektlar va sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish  asosida foydalanishlarni boshqaradi. | ABAC |
| 182 | XACML foydalanishni boshqarishni qaysi  usulining standarti? | ABAC |
| 183 | Biometrik autentifikatsiyalash usullari an’anaviy  usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan? | barchasi |
| 184 | Axborotning kriptografik himoya vositalari necha  turda? | 3 |
| 185 | Dasturiy shifrlash vositalari necha turga bo‘linadi | 4 |
| 186 | Diskni shifrlash nima uchun amalga oshiriladi? | Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun  amalga oshiriladi |
| 187 | Ma’lumotlarni yo‘q qilish odatda necha hil  usulidan foydalaniladi? | 4 |
| 188 | Kompyuter tarmoqlari bu – | Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan  kompyuterlar guruhi |
| 189 | Tarmoq modeli –bu.. ikki | Hisoblash tizimlariorasidagi aloqani ularning ichki tuzilmaviy vatexnologik asosidan qat’iy  nazar muvaffaqqiyatli o‘rnatilishini asosidir to‘plami |
| 190 | OSI modelida nechta tarmoq sathi bor | 7 |
| 191 | OSI modeli 7 stahi bu | Ilova |

|  |  |  |
| --- | --- | --- |
| 192 | OSI modeli 1 stahi bu | Fizik |
| 193 | OSI modeli 2 stahi bu | Kanal |
| 194 | TCP/IP modelida nechta satx mavjud | 4 |
| 195 | Qanday tarmoq qisqa masofalarda qurilmalar  o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi. | Shaxsiy tarmoq |
| 196 | Tarmoq kartasi bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash  imkoniyatini taqdim etadi. |
| 197 | Switch bu... | Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili  keltirilgan portga uzatadi |
| 198 | Hab bu... | ko‘plab tarmoqlarni ulash uchun yoki LAN  segmentlarini bog‘lash uchun xizmat qiladi. |
| 199 | Tarmoq repiteri bu... | Signalni tiklash yoki qaytarish uchun  foydalaniladi. |
| 200 | Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini  amalga oshiradi. | DNS tizimlari |
| 201 | ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq  ulanishlarini sozlashga yordam beradi. | TCP |
| 202 | …. protokolidan odatda o‘yin va video ilovalar  tomonidan keng foydalaniladi. | UDP |
| 203 | Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil  ma’lumotlari bilan ta’minlaydi. | IP |
| 204 | Tarmoq taxdidlari necha turga bo‘linadi | 4 |
| 205 | Qanday xujum asosiy hujumlarni oson amalga  oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; | Razvedka hujumlari |
| 206 | Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat  qiladi | Kirish hujumlari |
| 207 | Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud  bo‘lgan biror xizmatni cheklashga urinadi; | Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari |
| 208 | Qanday xujumdp zararli hujumlar tizim yoki  tarmoqqa bevosita va bilvosita ta’sir qiladi; | Zararli hujumlar |
| 209 | Elektron raqamli imzo algoritmi qanday  bosqichlardan iborat bo‘ladi? | Imzo qo‘yish va imzoni tekshirishdan |
| 210 | Imzoni haqiqiyligini tekshirish qaysi kalit  yordamida amalga oshiriladi? | Imzo muallifining ochiq *kaliti yordamida* |
| 211 | Tarmoq modeli-bu... | Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik  asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir |
| 212 | OSI modeli nechta sathga ajraladi? | 7 |
| 213 | Fizik sathning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
| 214 | Ilova sathning vazifasi nimadan iborat | Ilovalarni tarmoqqa ulanish jarayoni |

|  |  |  |
| --- | --- | --- |
| 215 | Kanal sathning vazifasi nimadan iborat | Fizik manzillash |
| 216 | Tarmoq sathning vazifasi nimadan iborat | Yo‘lni aniqlash va mantiqiy manzillash |
| 217 | TCP/IP modeli nechta sathdan iborat | 4 |
| 218 | Quyidagilarninf qaysi biri Kanal sathi protokollari | Ethernet, Token Ring, FDDI, X.25, Frame  Relay, RS-232, v.35. |
| 219 | Quyidagilarninf qaysi biri tarmoq sathi  protokollari | . IP, ICMP, ARP, RARP |
| 220 | Quyidagilarninf qaysi biri transport sathi  protokollari | TCP, UDP, RTP |
| 221 | Quyidagilarninf qaysi biri ilova sathi protokollari | HTTP, Telnet, FTP, TFTP, SNMP, DNS,  SMTP va hak |
| 222 | TCP/IP modelining kanal sathiga OSI modelining  qaysi sathlari mos keladi | Kanal, Fizik |
| 223 | TCP/IP modelining tarmoq sathiga OSI  modelining qaysi sathlari mos keladi | Tarmoq |
| 224 | TCP/IP modelining transport sathiga OSI  modelining qaysi sathlari mos keladi | Tramsport |
| 225 | TCP/IP modelining ilova sathiga OSI modelining  qaysi sathlari mos keladi | Ilova, taqdimot, seans |
| 226 | Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan  qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
| 227 | Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang. | . Odatda ijaraga olingan telekommunikatsiya  liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi. |
| 228 | Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang. | Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda  tutadi |
| 229 | Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang. | Qisqa masofalarda qurilmalar o‘rtasida  ma’lumot almashinish imkoniyatini taqdim etadi |
| 230 | Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun  markaziy tugunga individual bog‘langan bo‘ladi |
| 231 | Quyidagilardan qaysi biri tarmoqning shina  topologiyasiga berilgan | Tarmoqda yagona kabel barcha  kompyuterlarni o‘zida birlashtiradi |
| 232 | Quyidagilardan qaysi biri tarmoqning halqa  topologiyasiga berilgan | Yuboriluvchi va qabul qilinuvchi ma’lumot  TOKYeN yordamida manziliga yetkaziladi |
| 233 | Quyidagilardan qaysi biri tarmoqning mesh  topologiyasiga berilgan | Tarmoqdagi barcha kompyuter va tugunlar  bir-biri bilan o‘zaro bog‘langan bo‘ladi |
| 234 | Tarmoq kartasi nima? | Hisoblash qurilmasining ajralmas qismi  bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
| 235 | Repetir nima? | Odatda signalni tiklash yoki qaytarish uchun  foydalaniladi |
| 236 | Hub nima? | Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni  ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi |
| 237 | Switch nima? | Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.  Qabul qilingan signalni barcha chiquvchi |

|  |  |  |
| --- | --- | --- |
|  |  | portlarga emas balki paketda manzili  keltirilgan portga uzatadi |
| 238 | Router nima? | Qabul qilingan ma’lumotlarni tarmoq sathiga  tegishli manzillarga ko‘ra (IP manzil) uzatadi |
| 239 | DNS tizimlari. | Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini  amalga oshiradi |
| 240 | TCP bu- … | Transmission Control Protocol |
| 241 | UDP bu-… | User datagram protocol |
| 242 | Tarmoq xavfsizligiga tahdidlar tavsiflangan  bandni belgilang | Ichki, tashqi |
| 243 | Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib  keladi | Biznes jarayonlarni to‘xtab qolishiga olib keladi |
| 244 | Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi | Hujum natijasida ishlab chiqarishi yo‘qolgan hollarda uni qayta tiklash ko‘p vaqt talab  qiladi va bu vaqtda ishlab chiqarish to‘xtab qoladi |
| 245 | Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib  keladi | Konfidensial axborotni chiqib ketishi natijasida, tashkilot shaxsiy ma’lumotlarini  yo‘qolishi mumkin |
| 246 | Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib  keladi | Tashkilot xodimlarining shaxsiy va ishga oid ma’ulmotlarini kutilmaganda oshkor bo‘lishi  ushbu xodimlarga bevosita ta’sir qiladi |
| 247 | Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha  bardoshli bo‘lmasligi |
| 248 | Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi | tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish,  parollarni noto‘g‘ri boshqarilishi |
| 249 | Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. | Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab  chiqilgani sabab bo‘ladi. |
| 250 | Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan  tarmoq hujumi qaysi | Razvedka hujumlari |
| 251 | Ma’lumotlarni zaxira nusxalash bu – … | Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini  beradi |
| 252 | Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash  uchun qanday amaldan foydalanamiz | Zaxira nusxalash |
| 253 | Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar  bazasini xatolik bilan boshqarilganligi. |
| 254 | Zahira nusxalash strategiyasi nechta bosqichni o’z  ichiga oladi? | 5 |

|  |  |  |
| --- | --- | --- |
| 255 | Zaxiralash uchun zarur axborotni aniqlash nechta  bosqichda amalga oshiriladi. | 4 |
| 256 | Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos  bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
| 257 | RAID texnologiyasining transkripsiyasi qanday. | Random Array of Independent Disks |
| 258 | RAID texnologiyasida nechta satx mavjud | 6 |
| 259 | OSI modelining birinchi sathi qanday nomlanadi | Fizik sath |
| 260 | OSI modelining ikkinchi sathi qanday nomlanadi | Kanal sathi |
| 261 | OSI modelining uchinchi sathi qanday nomlanadi | Tarmoq sathi |
| 262 | OSI modelining oltinchi sathi qanday nomlanadi | Taqdimlash sathi |
| 263 | OSI modelining ettinchi sathi qanday nomlanadi | Amaliy sath |
| 264 | Elektr signallarini qabul qilish va uzatish  vazifalarini OSI modelining qaysi sathi bajaradi | Fizik sath |
| 265 | Keltirilgan protokollarning qaysilari transport  sathi protokollariga mansub | TCP,UDP |
| 266 | OSI modelining fizik sathi qanday funktsiyalarni  bajaradi | Elektr signallarini uzatish va qabul qilish |
| 267 | OSI modelining amaliy sathi qanday  funktsiyalarni bajaradi | Klient dasturlari bilan o’zaro muloqotda  bo’lish |
| 268 | 12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan  sonlar soni nechta? | 8 ta |
| 269 | Yevklid algoritmi qanday natijani beradi? | Sonning eng katta umumiy bo’luvchisini  toppish |
| 270 | Qanday sonlar tub sonlar deb yuritiladi? | Faqatgina 1 ga va o’ziga bo’linadigan sonlar  tub sonlar deyiladi. |
| 271 | To‘liq zaxiralash | To‘liq va o‘sib boruvchi usullarning mujassamlashgan ko‘rinishi bo‘lib, oxirgi zaxiralangan nusxadan boshlab bo‘lgan o‘zgarishlarni zaxira nusxalab boradi. • Amalga oshirish to‘liq zaxiralashga qaraganda tez amalga oshiriladi. • Qayta tiklash o‘sib boruvchi zaxiralashga qaraganda tez amalga oshiriladi. • Ma’lumotni saqlash  uchun to‘liq zaxiralashga qaraganda kam joy talab etadi |
| 272 | O‘sib boruvchi zaxiralash | Zaxiralangan ma’lumotga nisbatan o‘zgarish yuz berganda zaxirilash amalga oshiriladi. • Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usuli bo‘lishi mumkin (to‘liq saxiralashdan). • Saqlash uchun kam hajm va  amalga oshirish jarayoni tez |
| 273 | Differensial zaxiralash | Ushbu zaxiralashda tarmoqga bog‘lanishamalga oshiriladi. • Iliq zaxiralashda, tizim yangilanishi davomiy  yangilanishni qabul qilish uchun ulanadi |
| 274 | Ushbu jarayon ma’lumot qanday yo‘qolgani, ma’lumotni qayta tiklash dasturiy vositasi va  ma’lumotni tiklash manzilini qayergaligiga bog‘liq bo‘ladi. Qaysi jarayon | Ma’lumotlarni qayta tiklash |
| 275 | Antivirus dasturlarini ko’rsating? | Drweb, Nod32, Kaspersky |

|  |  |  |
| --- | --- | --- |
| 276 | Wi-Fi tarmoqlarida quyida keltirilgan qaysi  shifrlash protokollaridan foydalaniladi | wep, wpa, wpa2 |
| 277 | Axborot himoyalangan qanday sifatlarga ega  bo’lishi kerak? | ishonchli, qimmatli va to’liq |
| 278 | Axborotning eng kichik o’lchov birligi nima? | bit |
| 279 | Virtual xususiy tarmoq – bu? | VPN |
| 280 | Xavfli viruslar bu - … | kompyuter ishlashida jiddiy nuqsonlarga  sabab bo’luvchi viruslar |
| 281 | Mantiqiy bomba – bu … | Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning  alohida modullari |
| 282 | Rezident virus... | tezkor xotirada saqlanadi |
| 283 | DIR viruslari nimani zararlaydi? | FAT tarkibini zararlaydi |
| 284 | .... kompyuter tarmoqlari bo’yicha tarqalib, komlg’yuterlarning tarmoqdagi manzilini  aniqlaydi va u yerda o’zining nusxasini qoldiradi | «Chuvalchang» va replikatorli virus |
| 285 | Mutant virus... | shifrlash va deshifrlash algoritmlaridan  iborat- to’g’ri javob |
| 286 | Fire Wall ning vazifasi... | tarmoqlar orasida aloqa o’rnatish jarayonida  tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi |
| 287 | Kompyuter virusi nima? | maxsus yozilgan va zararli dastur |
| 288 | Kompyuterning viruslar bilan zararlanish  yo’llarini ko’rsating | disk, maxsus tashuvchi qurilma va kompyuter  tarmoqlari orqali |
| 289 | Troyan dasturlari bu... | virus dasturlar |
| 290 | Kompyuter viruslari xarakterlariga nisbatan necha  turga ajraladi? | 5 |
| 291 | Antiviruslarni, qo’llanish usuliga ko’ra... turlari  mavjud | detektorlar, faglar, vaktsinalar, privivkalar,  revizorlar, monitorlar |
| 292 | Axborotni himoyalash uchun ... usullari  qo’llaniladi. | kodlashtirish, kriptografiya, stegonografiya |
| 293 | Stenografiya mahnosi... | sirli yozuv |
| 294 | …sirli yozuvning umumiy nazariyasini yaratdiki,  u fan sifatida stenografiyaning bazasi hisoblanadi | K.Shennon |
| 295 | Kriptologiya yo’nalishlari nechta? | 2 |
| 296 | Kriptografiyaning asosiy maqsadi... | maxfiylik, yaxlitlilikni ta`minlash |
| 297 | Zararli dasturiy vositalarni aniqlash turlari nechta | 3 |
| 298 | Signaiurana asoslangan | ...bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura  sifatida xizmat qilishi mumkin. |
| 299 | O‘zgarishni aniqlashga asoslangan | Zararli dasturlar biror joyda joylashishi sababli, agar tizimdagi biror joyga o‘zgarishni aniqlansa, u holda u zararlanishni ko‘rsatishi  mumkin |
| 300 | Anomaliyaga asoslangan | Noodatiy yoki virusga o‘xshash yoki potensial zararli harakatlari yoki  xususiyatlarni topishni maqsad qiladi |
| 301 | Antiairuslar qanday usulda viruslarni aniqlaydi | Signaturaga asoslangan |
| 302 | Viruslar - | o‘zini o‘zi ko‘paytiradigan programma bo‘lib,  o‘zini boshqa programma ichiga, |

|  |  |  |
| --- | --- | --- |
|  |  | kompyuterning yuklanuvchi sektoriga yoki  hujjat ichiga biriktiradi |
| 303 | Rootkitlar- | ushbu zararli dasturiy vosita operatsion tizim  tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi |
| 304 | Backdoorlar - | zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi,  maslan, administrator parolisiz imtiyozga ega bo‘lish |
| 305 | Troyan otlari- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat  bo‘ladi |
| 306 | Ransomware- | mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni  shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi |
| 307 | Resurslardan foydalanish usuliga ko’ra viruslar  qanday turlarga bo’linadi | Virus parazit, Virus cherv |
| 308 | Zararlagan obyektlar turiga ko’ra | Dasturiy, yuklanuvchi, Makroviruslar,  multiplatformali viruslar |
| 309 | Faollashish prinspiga ko’ra | Resident, Norezident |
| 310 | Dastur kodini tashkil qilish yondashuviga ko‘ra | Shifrlangan, shifrlanmagan, Polimorf |
| 311 | Shifrlanmagan viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha  ishlashlar mavjud bo‘lmaydi. |
| 312 | P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang | 840 |
| 313 | 256mod25=? | 6 |
| 314 | bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki  o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi. | Tizim |
| 315 | Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi  yuqori sathli hujjat yoki hujjatlar to‘plami nima duyidadi | Xavfsizlik siyosati |
| 316 | RSA shifrlash algoritmida foydalaniladigan  sonlarning spektori o‘lchami qanday? | *p* va *q* –sonlarning ko‘paytmasini ifodalovchi  sonning spektoriga teng; |
| 317 | DES algoritmi akslantirishlari raundlari soni  qancha? | 16; |
| 318 | DES algoritmi shifrlash blokining chap va o‘ng  qism bloklarining o‘lchami qancha? | CHap qism blok 32 bit, o‘ng qism blok 32 bit; |
| 319 | Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli  tomonlari bor? | SHifrlash va deshifrlash jarayonlari uchun kalitlarni generatsiya qilish qoidalariga ko‘ra  farqlanadi |
| 320 | 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan  sonlar soni nechta? | 18 ta |
| 321 | 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan  sonlar soni nechta? | 4 ta |
| 322 | Eyler funsiyasida 𝜙(1) qiymati nimaga teng? | 0 |
| 323 | Eyler funksiyasida 60 sonining qiymatini toping. | 59 |

|  |  |  |
| --- | --- | --- |
| 324 | Eyler funksiyasi yordamida 1811 sonining  qiymatini toping. | 1810 |
| 325 | 97 tub sonmi? | Tub |
| 326 | Quyidagi modulli ifodani qiymatini toping (148 +  14432) mod 256. | 244 |
| 327 | Quyidagi sonlarning eng katta umumiy  bo’luvchilarini toping. 88 i 220 | 44 |
| 328 | Quyidagi ifodani qiymatini toping. -17mod11 | 5 |
| 329 | 2 soniga 10 modul bo’yicha teskari sonni toping. | Ø |
| 330 | Tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta’minlash sohasidagi tadbirlar  tavsiflanadigan yuqori darajadagi reja nima? | Kiberxavfsizlik siyosati |
| 331 | Kiberxavfsizlik siyosati tashkilotda nimani  ta’minlaydi? | tashkilot masalalarini yechish himoyasini  yoki ish jarayoni himoyasini ta’minlaydi |
| 332 | Kiberxavfsizlikni ta’minlash masalalari bo’yicha  xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang | SANS (System Administration Networking and Security) |
| 333 | Korxonaning davomli muvaffaqiyat bilan faoliyat yuritishini ta’minlashga mo’ljallangan strukturalangan va o’zaro bog’langan harakatlar  to’plami- … | Strategiya |
| 334 | Tahdidlarning muvaffaqiyatli amalga oshirilishiga  imkon beruvchi har qanday omil – bu … | Zaiflik |
| 335 | ISO/IEC 27002:2005 – …. | Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini  boshqarishning amaliy qoidalari |
| 336 | O’zDStISO/IEC 27005:2013 – …. | Axborot texnologiyasi. Xavfsizlikni  ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish |
| 337 | Axborot xavfsizligi arxitekturasining nechta satxi  bor? | 3 |
| 338 | Rahbariy hujjat. Ma’lumotlar uzatish tarmog’ida axborot xavfsizligini ta’minlash to’g’risida Nizom  - Xujjat raqamini toping | RH 45-215:2009 |
| 339 | Davlat hokimiyati va boshqaruv organlarining  axborot xavfsizligini ta’minlash dasturini ishlab chiqish tartibi - Xujjat raqamini toping | RH 45-185:2011 |
| 340 | Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta’minlash darajasini  aniqlash tartibi - Xujjat raqamini toping | RH 45-193:2007 |
| 341 | Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta’riflar - Xujjat raqamini  toping | TSt 45-010:2010 |
| 342 | Quyidagilardan qaysi standart aloqa va  axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta’riflarni belgilaydi? | TSt 45-010:2010 |
| 343 | Sub’ekt identifikatorini tizimga yoki talab qilgan  sub’ektga taqdim qilish jarayoni nima? | Identifikatsiya |

|  |  |  |
| --- | --- | --- |
| 344 | Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash  jarayoni nima? | Autentifikatsiya |
| 345 | Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni – nima  deyiladi? | Avtorizatsiya |
| 346 | Identifikatsiya nima? | Sub’ekt identifikatorini tizimga yoki talab  qilgan sub’ektga taqdim qilish jarayoni |
| 347 | Autentifikatsiya nima? | Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati  mavjudligini aniqlash jarayoni |
| 348 | Avtorizatsiya nima? | Identifikatsiya va autentifikatsiyadan o’tgan  foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni |
| 349 | ... - Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o’tishni  ta’minlovchi biror axborot | Parol |
| 350 | Smart karta o’lchamidagi, kichik xajmdagi xotira va xisoblash imkoniyatiga ega bo’lgan, o’zida parol yoki kalitni saqlovchi qurilma nima deb  ataladi? | Token, Smartkarta |
| 351 | Smarkarta nima asosida autentifikatsiyalaydi? | Something you have |
| 352 | Faqat bir marta foydalaniluvchi, xar bir sessiya  uchun o’zgarib turadigan parol nima deyiladi? | One-time password (OTP) |
| 353 | Foydalanuvchining tarmoqdagi harakatini, shu  jumladan, uning resurslardan foydalanishga urinishini qayd etish nima deb ataladi? | Ma’murlash |
| 354 | Amaldagi qonunchilikka mos ravishda texnik, dasturiy va dasturiy-texnik vositalar yordamida axborot xavfsizligining nokriptografik usullari bilan ta’minlashni inobatga oluvchi axborot  himoyasi nima? | Axborotning texnik himoyasi |
| 355 | Nazorat hududi – bu ... | Qo’riqlanuvchi soha bo’lib, uning ichida kommunikatsiya qurilmalari hamda axborot tarmog’ining lokal tarkibiy qurilmalarini  birlashtiruvchi barcha nuqtalar joylashadi |
| 356 | Texnik himoya vositalari – bu ... | Texnik qurilmalar, komplekslar yoki tizimlar  yordamida ob’ektni himoyalashdir |
| 357 | Bu axborotni tutib olish qurilmasi bo’lib, ularda  uzatuvchi qurilma sifatida kontaktli mikrofonlardan foydalaniladi | Stetoskoplar |
| 358 | Xesh funktsiya to’g’ri ko’rsatilgan javobni  aniqlang. | MD5 |
| 359 | MD5, SHA1, Tiger xesh funktsiyalari uchun blok  uzunligi necha baytga teng? | 64 bayt |
| 360 | Sub’ektni ob’ektga ishlash qobilyatini aniqlash –  nima? | Foydalanishni boshqarish |
| 361 | Foydalanishni boshqarishda sub’ekt bu - .... | Inson, dastur, jarayon |
| 362 | Foydalanishni boshqarishning qaysi usuli  tizimdagi shaxsiy ob’ektlarni ximoyalash uchun qo’llaniladi? | Discretionary access control DAC |

|  |  |  |
| --- | --- | --- |
| 363 | Foydalanishni boshqarishning qaysi usulidan  asosan operatsion tizimlarda qo’llaniladi? | Discretionary access control DAC |
| 364 | Foydalanishni boshqarishning qaysi usulida  foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi? | Mandatory access control MAC |
| 365 | Foydalanishni boshqarishning qaysi usulida  xavfsizlik markazlashgan tarzda xavfsizlik siyosati m’muri tomonidan amalga oshiriladi? | Mandatory access control MAC |
| 366 | Foydalanishni boshqarishning qaysi usulida xar bir foydalanuvchini foydalanish ruxsatini  belgilash o’rniga rol uchun ob’ektlardan foydalanish ruxsatini ko’rsatish yetarli bo’ladi? | Role-based access control RBAC |
| 367 | Foydalanishni boshqarishning qaysi usulida  sub’ekt va ob’ektlarga tegishli xuquqlarni ma’murlash oson kechadi? | Role-based access control RBAC |
| 368 | Firibgarlikni oldini olish uchun bir shaxs tomonidan ko’plab vazifalarni bajarishga ruxsat bermaslik zarur. Bu muammo foydalanishni  boshqarishni qaysi usulida bartaraf etiladi? | Role-based access control RBAC |
| 369 | Ob’ekt va sub’ektlarning attributlari, ular bilan mumkin bo’lgan amallar va so’rovlarga mos keladigan muxit uchun qoidalarni taxlil qilish  asosida foydalanishni boshqarish - .... | Attribute based access control ABAC |
| 370 | Attribute based access control ABAC usuli  attributlari qaysilar? | Foydalanuvchi attributlari, Resurs attributlari,  Ob’ekt va muxit attributlari |
| 371 | Foydalanishni boshqarishning qaysi usulida ruxsatlar va xarakatni kim bajarayotganligi to’g’risidagi xolatlar “agar, u xolda” buyrug’idan  tashkil topgan qoidalarga asoslanadi? | Attribute based access control ABAC |
| 372 | XASML standarti foydalanishni boshqarishning  qaysi usulida qo’llaniladi? | Attribute based access control ABAC |
| 373 | XASML standartida qoida nima? | Maqsad, ta’sir, shart, majburiyat va  maslaxatlar |
| 374 | XASML standartida maqsad nima? | Sub’ekt ob’ekt ustida nima xarakat qilishi |
| 375 | Lampsonning foydalanishni boshqarish matritsasi  nimalardan tashkil topgan? | Imtiyozlar ro’yxati |
| 376 | Access control list va Capability list bu nimaning  asosiy elementi xisoblanadi? | Lampson matritsasining |
| 377 | Lampson matritsasining satrlarida nima  ifodalanadi? | Sub’ektlar |
| 378 | Foydalanishni boshqarishning mantiqiy vositalari  infratuzilma va uning ichidagi tizimlarda ... uchun foydalaniladi. | Mandat, Tasdiqlash, Avtorizatsiya |
| 379 | SHaxsiy simsiz tarmoq standartini aniqlang. | Bluetooth, IEEE 802.15, IRDA |
| 380 | Lokal simsiz tarmoq standartini aniqlang. | IEEE 802.11, Wi-Fi, HiperLAN |
| 381 | Regional simsiz tarmoq standartini aniqlang. | IEEE 802.16, WiMAX |
| 382 | Global simsiz tarmoq standartini aniqlang. | CDPD, 2G, 2.5G, 3G, 4G, 5G |
| 383 | Bluetooth, IEEE 802.15, IRDA standartida  ishlovchi simsiz tarmoq turini aniqlang. | SHaxsiy simsiz tarmoq |
| 384 | IEEE 802.11, Wi-Fi, HiperLAN standartida  ishlovchi simsiz tarmoq turini aniqlang. | Lokal simsiz tarmoq |

|  |  |  |
| --- | --- | --- |
| 385 | IEEE 802.16, WiMAX standartida ishlovchi  simsiz tarmoq turini aniqlang. | Regional simsiz tarmoq |
| 386 | CDPD, 2G, 2.5G, 3G, 4G, 5G standartida  ishlovchi simsiz tarmoq turini aniqlang. | Global simsiz tarmoq |
| 387 | Bluetooth qanday chastota oralig’ida ishlaydi? | 2.4-2.485 Ggts |
| 388 | Wi-Fi qanday chastota oralig’ida ishlaydi? | 2.4-5 Ggts |
| 389 | WiMax tarmog’ining tezligi qancha? | 1 Gbit/sekund |
| 390 | Quyidagilardan qaysi biri MITM xujumiga  tegishli xatti-xarakat ximoblanadi? | Aloqa seansini konfidentsialligini va  yaxlitligini buzish |
| 391 | WiMAX tarmoq arxitekturasi nechta tashkil  etuvchidan iborat? | 5 |
| 392 | WiMAX tarmoq arxitekturasi qaysi tashkil  etuvchidan iborat? | Base station, Subscriber station, Mobile  station, Relay station, Operator network |
| 393 | GSM raqamli mobil telefonlarining nechanchi  avlodi uchun ishlab chiqilgan protokol? | Ikkinchi avlodi |
| 394 | GSM standarti qaysi tashkilot tomonidan ishlab  chiqilgan? | European telecommunications standards  institute |
| 395 | .... – o’zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma’lumoti va xavfsizlik  algoritmlarini saqlaydi. | Sim karta |
| 396 | Rutoken S qurilmasining og’irligi qancha? | 6.3 gramm |
| 397 | True Crypt dasturi qaysi algoritmlardan  foydalanib shifrlaydi? | AES, Serpent, Twofish |
| 398 | Ma’lumotni saqlash vositalarida saqlangan  ma’lumot konfidentsialligini aniqlash qaysi dasturiy shifrlash vositalarining vazifasi? | Disc encryption software |
| 399 | BestCrypt dasturi qaysi algoritmlardan foydalanib  shifrlaydi? | AES, Serpent, Twofish |
| 400 | AxCrypt dasturi qaysi algoritmlardan foydalanib  shifrlaydi? | AES-256 |
| 401 | Qog’oz ko’rinishidagi axborotlarni yo’q qilish  qurilmasining nomini kiriting. | Shreder |
| 402 | Ma’lumotlarni bloklarga bo’lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini  yozish qaysi texnologiya? | RAID 0 |
| 403 | Qaysi texnologiyada ma’lumotni ko’plab  nusxalari bir vaqtda bir necha disklarga yoziladi? | RAID 1 |
| 404 | Qaysi texnologiyada ma’lumotlarni bir necha  disklarda bayt satxida ajratilgan xolda yoziladi? | RAID 3 |
| 405 | Qaysi texnologiyada ma’lumotlarni bir necha  disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi? | RAID 5 |
| 406 | Disk zararlanganda “qaynoq almashtirish” yordamida uni almashtirish mumkin. Bu xususiyat  qaysi texnologiyaga tegishli? | RAID 50 |
| 407 | Zaxiralashning qanday turlari mavjud? | To’liq, o’sib boruvchi, differentsial |
| 408 | IOS, Android, USB xotiralardan ma’lumotlarni  tiklash uchun qaysi dasturdan foydalaniladi? | EASEUS Data recovery wizard |
| 409 | Foydalanuvchi ma’lumotlarini qo’lga kirituvchi  va uni xujumchiga yuboruvchi dasturiy kod nima? | Spyware |

|  |  |  |
| --- | --- | --- |
| 410 | Operatsion tizim tomonidan aniqlanmasligi uchun  ma’lum xarakatlarni yashirish nima deyiladi? | Rootkits |
| 411 | Qurbon kompyuterda mavjud qimmatli fayllarni  shifrlaydi yoki qulflab qo’yib to’lov amalga oshirishni talab qiladi. Bu qaysi zararli dastur? | Ransomware |
| 412 | Quyidagilardan o’zidan ko’payishi yo’q  bo’lganlarini belgilang. | Mantiqiy bomba, Troyan oti, Backdoors |
| 413 | Viruslar resurslardan foydalanish usuliga ko’ra  qanday turlarga bo’linadi? | Virus parazitlar, virus chervlar |
| 414 | Viruslar zararlangan ob’ektlar turiga ko’ra qanday  turlarga bo’linadi? | Dasturiy, yuklanuvchi, makroviruslar, ko’p  platformali |
| 415 | Viruslar faollashish printsipiga ko’ra qanday  turlarga bo’linadi? | Rezident, norezident |
| 416 | Viruslar dastur kodini tashkil qilish yondoshuviga  ko’ra qanday turlarga bo’linadi? | SHifrlangan, shifrlanmagan, polimorf |
| 417 | Dastlabki virus nechanchi yilda yaratilgan? | 1988 |
| 418 | ILOVEYOU virusi keltirgan zarar qancha? | 10 mlrd. Dollar |
| 419 | CodeRed virusi keltirgan zarar qancha? | 2 mlrd. Dollar |
| 420 | Melissa virusi keltirgan zarar qancha? | 80 million dollar |
| 421 | NetSky virusi keltirgan zarar qancha? | 18 mlrd. Dollar |
| 422 | MyDoom virusi keltirgan zarar qancha? | 38 mlrd. Dollar |
| 423 | Risk monitoring ….. ni paydo bo’lish  imkoniyatini aniqlaydi. | Yangi risklar |
| 424 | ….. riskni tutuvchi mos nazorat usuli amalga  oshirilganligini kafolatlaydi. | Risk monitoring |
| 425 | Axborot xavfsizligi siyoatining necha hil turi bor? | 3 |
| 426 | Internetdan foydalanish siyosatining nechta turi  mavjud? | 4 |
| 427 | Nomuntazam siyosat (Promiscuous Policy) nima? | Tizim resurslaridan foydalanishda hech  qanday cheklovlar qo’ymaydi |
| 428 | Paranoid siyosati (Paranoid Policy) – bu …. | Hamma narsa ta’qiqlanadi |
| 429 | Ruxsat berishga asoslangan siyosat (Permissive  Policy) – bu … | Faqat ma’lum hizmatlar/hujumlar/harakatlar  bloklanadi |
| 430 | Ehtiyotkorlik siyosati (Prudent Policy) – bu …. | Barcha hizmatlar blokirovka qilingandan  so’ng bog’lanadi |
| 431 | Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi. Bu qaysi xavfsizlik  siyosatiga hos? | Nomuntazam siyosat (Promiscuous Policy) |
| 432 | Barcha hizmatlar blokirovka qilingandan so’ng  bog’lanadi. Bu qaysi xavfsizlik siyosatiga hos? | Ehtiyotkorlik siyosati (Prudent Policy) |
| 433 | Faqat ma’lum hizmatlar/hujumlar/harakatlar  bloklanadi. Bu qaysi xavfsizlik siyosatiga hos? | Ruxsat berishga asoslangan siyosat  (Permissive Policy) |
| 434 | Hamma narsa ta’qiqlanadi. Bu qaysi xavfsizlik  siyosatiga hos? | Paranoid siyosati (Paranoid Policy) |
| 435 | Tizim arxitekturasining turlari nechta? | 5 |
| 436 | Internet, havo hujumidan mudofaa, transport  tizimlari qaysi tizim arxitekturasiga xos? | Hamkorlik tizimlari arxitekturasi |
| 437 | Cloud computing texnologiyasining nechta asosiy  turi mavjud? | 3 |
| 438 | Raqamli soatlar qaysi texnologiyaga tegishli? | O’rnatilgan tizimlar (Embedde systems) |

|  |  |  |
| --- | --- | --- |
| 439 | Xavfsizlikning asosiy yo’nalishlarini sanab o’ting. | \*Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik,  Ekologik xavfsizlik |
| 440 | Axborot xavfsizligining asosiy maqsadlaridan  biri- bu… | \*Axborotlarni o’g’irlanishini, yo’qolishini,  soxtalashtirilishini oldini olish |
| 441 | Konfidentsiallikga to’g’ri ta`rif keltiring. | \*axborot inshonchliligi, tarqatilishi mumkin  emasligi, maxfiyligi kafolati; |
| 442 | Yaxlitlikni buzilishi bu - … | \*Soxtalashtirish va o’zgartirish |
| 443 | ... axborotni himoyalash tizimi deyiladi. | \*Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va  choralarning kompleksi |
| 444 | Kompyuter virusi nima? | \*maxsus yozilgan va zararli dastur |
| 445 | Axborotni himoyalash uchun ... usullari  qo’llaniladi. | \*kodlashtirish, kriptografiya, stegonografiya |
| 446 | Stenografiya ma’nosi... | \*sirli yozuv |
| 447 | Kriptografiyaning asosiy maqsadi... | \*maxfiylik, yaxlitlilikni ta`minlash |
| 448 | SMTP - Simple Mail Transfer protokol nima? | \*elektron pochta protokoli |
| 449 | SKIP protokoli... | \*Internet protokollari uchun  kriptokalitlarning oddiy boshqaruvi |
| 450 | Kompyuter tarmog’ining asosiy komponentlariga  nisbatan xavf-xatarlar… | \*uzilish, tutib qolish, o’zgartirish,  soxtalashtirish |
| 451 | ...ma`lumotlar oqimini passiv hujumlardan  himoya qilishga xizmat qiladi. | \*konfidentsiallik |
| 452 | Foydalanish huquqini cheklovchi matritsa modeli  bu... | \*Bella La-Padulla modeli |
| 453 | Kompyuter tarmoqlarida tarmoqning  uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? | \*TCP/IP, X.25 protokollar |
| 454 | Himoya tizimi kompleksligiga nimalar orqali erishiladi? | \*Xuquqiy tashkiliy, muhandis, texnik va  dasturiy matematik elementlarning mavjudligi orqali |
| 455 | Kalit – bu … | \*Matnni shifrlash va shifrini ochish uchun  kerakli axborot |
| 456 | Qo’yish, o’rin almashtirish, gammalash  kriptografiyaning qaysi turiga bog’liq? | \*simmetrik kriptotizimlar |
| 457 | Autentifikatsiya nima? | \*Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini  tekshirish muolajasi |
| 458 | Identifikatsiya bu- … | \*Foydalanuvchini uning identifikatori (nomi)  bo’yicha aniqlash jarayoni |
| 459 | O’rin almashtirish shifri bu - … | \*Murakkab bo’lmagan kriptografik  akslantirish |
| 460 | Simmetrik kalitli shifrlash tizimi necha turga  bo’linadi. | \*2 turga |
| 461 | Kalitlar boshqaruvi 3 ta elementga ega bo’lgan  axborot almashinish jarayonidir bular … | \*hosil qilish, yig’ish, taqsimlash |
| 462 | Kriptologiya - | \*axborotni qayta akslantirib himoyalash  muammosi bilan shug’ullanadi |

|  |  |  |
| --- | --- | --- |
| 463 | Kriptografiyada alifbo – | \*axborot belgilarini kodlash uchun  foydalaniladigan chekli to’plam |
| 464 | Simmetrik kriptotizimlarda ... jumlani davom  ettiring | \*shifrlash va shifrni ochish uchun bitta va  aynan shu kalitdan foydalaniladi |
| 465 | Kriptobardoshlilik deb … | \*kalitlarni bilmasdan shifrni ochishga  bardoshlilikni aniqlovchi shifrlash tavsifi |
| 466 | Elektron raqamli imzo deb – | \*xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan  qo’shimcha |
| 467 | Kriptografiya – | \*axborotni qayta akslantirishning matematik  usullarini izlaydi va tadqiq qiladi |
| 468 | Kriptografiyada matn – | \*alifbo elementlarining tartiblangan to’plami |
| 469 | Kriptoanaliz – | \*kalitlarni bilmasdan shifrni ochishga  bardoshlilikni aniqlovchi shifrlash tavsifi |
| 470 | Shifrlash – | \*akslantirish jarayoni: ochiq matn deb  nomlanadigan matn shifrmatnga almashtiriladi |
| 471 | Kalit taqsimlashda ko’proq nimalarga e`tibor  beriladi? | \*Tez, aniq va maxfiyligiga |
| 472 | Faol hujum turi deb… | \*Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar  tayyorlash harakatlaridan iborat jarayon |
| 473 | Blokli shifrlash- | \*shifrlanadigan matn blokiga qo’llaniladigan  asosiy akslantirish |
| 474 | Simmetrik kriptotizmning uzluksiz tizimida … | \*ochiq matnning har bir harfi va simvoli  alohida shifrlanadi |
| 475 | Kripto tizimga qo’yiladigan umumiy talablardan  biri | \*shifr matn uzunligi ochiq matn uzunligiga  teng bo’lishi kerak |
| 476 | Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos? | \*Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa  deshifrlanadi |
| 477 | Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish  usulini belgilang | \*Vijener matritsasi, Sezar usuli |
| 478 | Akslantirish tushunchasi deb nimaga aytiladi? | \*1-to’plamli elementlariga 2-to’plam  elementalriga mos bo’lishiga |
| 479 | Simmetrik guruh deb nimaga aytiladi? | \*O’rin almashtirish va joylashtirish |
| 480 | Qo’yish, o’rin almashtirish, gammalash  kriptografiyaning qaysi turiga bog’liq? | \*simmetrik kriptosistemalar |
| 481 | Xavfli viruslar bu - … | \*kompyuter ishlashida jiddiy nuqsonlarga  sabab bo’luvchi viruslar |
| 482 | Mantiqiy bomba – bu … | \*Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning  alohida modullari |
| 483 | Elektron raqamli imzo tizimi qanday muolajalarni  amalga oshiradi? | \*raqamli imzoni shakllantirish va tekshirish  muolajasi |
| 484 | Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan  foydalaniladi? | \*Simmetrik va assimetrik |

|  |  |  |
| --- | --- | --- |
| 485 | Axborot himoyasi nuqtai nazaridan kompyuter  tarmoqlarini nechta turga ajratish mumkin? | \*Korporativ va umumfoydalanuvchi |
| 486 | Elektromagnit nurlanish va ta`sirlanishlardan  himoyalanish usullari nechta turga bo’linadi? | \*Sust va faol |
| 487 | Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan  foydalaniladi? | \*SMTP, POP yoki IMAR |
| 488 | Axborot resursi – bu? | \*axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar  bazasi |
| 489 | Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy  bo’lmagan qayd yozuvi – bu? | \*login |
| 490 | Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar  ketma-ketligi (maxfiy so’z) – bu? | \*parol |
| 491 | Identifikatsiya jarayoni qanday jarayon? | \* axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni  aniqlash jarayoni |
| 492 | Autentifikatsiya jarayoni qanday jarayon? | \*obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini  tekshirish orqali aslligini aniqlash |
| 493 | Avtorizatsiya jarayoni qanday jarayon? | \*foydalanuvchining resursdan foydalanish  huquqlari va ruxsatlarini tekshirish jarayoni |
| 494 | Ro’yxatdan o’tish bu? | \*foydalanuvchilarni ro’yxatga olish va ularga  dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni |
| 495 | Axborot qanday sifatlarga ega bo’lishi kerak? | \*ishonchli, qimmatli va to’liq |
| 496 | Axborotning eng kichik o’lchov birligi nima? | \*bit |
| 497 | Elektron hujjatning rekvizitlari nechta qismdan  iborat? | \*4 |
| 498 | Axborotlarni saqlovchi va tashuvchi vositalar  qaysilar? | \*fleshka, CD va DVD disklar |
| 499 | Imzo bu nima ? | \*hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan  insonning fiziologik xususiyati. |
| 500 | Muhr bu nima? | \*hujjatning haqiqiyligini va biror bir yuridik shaxsga tegishli ekanligini tasdiqlovchi  isbotdir |
| 501 | DSA – nima | \*Raqamli imzo algoritmi |
| 502 | El Gamal algoritmi qanday algoritm | \*Shifrlash algoritmi va raqamli imzo  algoritmi |
| 503 | Sezarning shifrlash sistemasining kamchiligi | \*Harflarning so’zlarda kelish chastotasini  yashirmaydi |
| 504 | Axborot xavfsizligi va xavfsizlik san’ati haqidagi  fan …. deyiladi? | \*Kriptografiya |

|  |  |  |
| --- | --- | --- |
| 505 | Tekstni boshqa tekst ichida ma’nosini yashirib  keltirish bu - | \*steganografiya |
| 506 | Shifrtekstni ochiq tekstga akslantirish jarayoni  nima deb ataladi? | \*Deshifrlash |
| 507 | …… – hisoblashga asoslangan bilim sohasi bo‘lib,  buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. | \*Kiberxavfsizlik |
| 508 | Risk | \*Potensial foyda yoki zarar |
| 509 | Tahdid nima? | \*Tashkilotga zarar yetkazishi mumkin  bo‘lgan istalmagan hodisa. |
| 510 | Kodlash nima? | \*Ma’lumotni osongina qaytarish uchun hammaga  ochiq bo‘lgan sxema yordamida  ma’lumotlarni boshqa formatga o‘zgartirishdir |
| 511 | Shifrlash nima? | Ma’lumotni osongina qaytarish uchun hammaga  ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir |
| 512 | Axborotni shifrni ochish (deshifrlash) bilan  qaysi fan shug’ullanadi | Kriptoanaliz |
| 513 | Qaysi juftlik RSA algoritmining ochiq va yopiq  kalitlarini ifodalaydi | {*d, e*} – ochiq, {*e, n*} – yopiq; |
| 514 | Zamonaviy kriptografiya qanday bo’limlardan  iborat? | Electron raqamli imzo; kalitlarni boshqarish |
| 515 | Kriptografik usullardan foydalanishning asosiy  yo’nalishlari nimalardan iborat? | uzatiliyotgan xabarlarni haqiqiyligini aniqlash |
| 516 | Shifr nima? | \* Shifrlash va deshifrlashda foydalaniladigan  matematik funktsiyadan iborat bo’lgan krptografik algoritm |
| 517 | Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? | \*Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq  kalitlardan foydalaniladi |
| 518 | Oqimli shifrlashning mohiyati nimada? | Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,  Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur, Oqimli shifrlash  algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi |
| 519 | Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating. | \*uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga  bog’liq bo’lishi lozim, |
| 520 | Kriptotizim qaysi komponentlardan iborat? | \*ochiq matnlar fazosi M, Kalitlar fazosi K, |

|  |  |  |
| --- | --- | --- |
|  |  | Shifrmatnlar fazosi C, Ek : M ® C (shifrlash  uchun) va Dk: C®M (deshifrlash uchun) funktsiyalar |
| 521 | Asimmetrik kriptotizimlar qanday maqsadlarda  ishlatiladi? | \*shifrlash, deshifrlash, ERI yaratish va  tekshirish, kalitlar almashish uchun |
| 522 | Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda  ishlatiladi. | \*ochiq kalitlar |
| 523 | Xesh-funktsiyani natijasi … | Kiruvchi xabar uzunligidan uzun xabar |
| 524 | RSA algoritmi qanday jarayonlardan tashkil  topgan | \*Kalitni generatsiyalash; Shifrlash;  Deshifrlash. |
| 525 | Ma’lumotlar butunligi qanday algritmlar orqali  amalga oshiriladi | \*Xesh funksiyalar |
| 526 | To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya  turiga mansub | \*Xalqa |
| 527 | Qaysi topologiya birgalikda foydalanilmaydigan  muhitni qo’llamasligi mumkin? | \*to’liq bog’lanishli |
| 528 | Kompyuterning tashqi interfeysi deganda nima tushuniladi? | \*kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish  qoidalari to’plamlari |
| 529 | Lokal tarmoqlarda keng tarqalgan topologiya turi  qaysi? | \*Yulduz |
| 530 | Ethernet kontsentratori qanday vazifani bajaradi | \*kompyuterdan kelayotgan axborotni qolgan  barcha kompyuterga yo’naltirib beradi |
| 531 | OSI modelida nechta satx mavjud | \*7 |
| 532 | OSI modelining to’rtinchi satxi qanday nomlanadi | \*Transport satxi |
| 533 | OSI modelining beshinchi satxi qanday  nomlanadi | \*Seanslar satxi |
| 534 | OSI modelining birinchi satxi qanday nomlanadi | \*Fizik satx |
| 535 | OSI modelining ikkinchi satxi qanday nomlanadi | \*Kanal satxi |
| 536 | OSI modelining uchinchi satxi qanday nomlanadi | \*Tarmoq satxi |
| 537 | OSI modelining oltinchi satxi qanday nomlanadi | \*Taqdimlash satxi |
| 538 | OSI modelining yettinchi satxi qanday nomlanadi | \*Amaliy satx |
| 539 | OSI modelining qaysi satxlari tarmoqqa bog’liq  satxlar hisoblanadi | \*fizik, kanal va tarmoq satxlari |
| 540 | OSI modelining tarmoq satxi vazifalari keltirilgan  qurilmalarning qaysi birida bajariladi | \*Marshrutizator |
| 541 | Elektr signallarini qabul qilish va uzatish  vazifalarini OSI modelining qaysi satxi bajaradi | \*Fizik satx |
| 542 | Ma’lumotlarni uzatishning optimal marshrutlarini  aniqlash vazifalarini OSI modelining qaysi satxi bajaradi | \*Tarmoq satxi |
| 543 | Keltirilgan protokollarning qaysilari tarmoq satxi  protokollariga mansub | \*IP, IPX |
| 544 | Keltirilgan protokollarning qaysilari transport  satxi protokollariga mansub | \*TCP,UDP |
| 545 | OSI modelining fizik satxi qanday funktsiyalarni  bajaradi | \*Elektr signallarini uzatish va qabul qilish |
| 546 | OSI modelining amaliy satxi qanday  funktsiyalarni bajaradi | \*Klient dasturlari bilan o’zaro muloqotda  bo’lish |

|  |  |  |
| --- | --- | --- |
| 547 | Keltirilgan protokollarning qaysilari kanal satxi  protokollariga mansub | \*Ethernet, FDDI |
| 548 | Keltirilgan protokollarning qaysilari taqdimlash  satxi protokollariga mansub | \*SNMP, Telnet |
| 549 | Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni  bu... | \*Avtorizatsiya |
| 550 | Autentifikatsiya faktorlari nechta | 4 |
| 551 | Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi  biror axborot nima | Login |
| 552 | Ko‘z pardasi, yuz tuzilishi, ovoz tembri- bular  autentifikatsiyaning qaysi faktoriga mos belgilar? | Biron nimaga egalik asosida |
| 553 | barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun  quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi? | \*Fizik satx |
| 554 | Fizik xavfsizlikda Yong‘inga qarshi tizimlar  necha turga bo‘linadi | \*2 |
| 555 | Avtorizatsiya tushunchasi odatda qaysi tushuncha  bilan sinonim sifatida ham foydalanadi? | \*Foydalanishni boshqarish |
| 556 | Foydalanishni boshqarish –bu... | Subyektni Subyektga ishlash qobilyatini  aniqlashdir. |
| 557 | Foydalanishni boshqarishda inson, dastur, jarayon  va xokazolar nima vazifani bajaradi? | Obyekt |
| 558 | Foydalanishna boshqarishda ma’lumot , resurs,  jarayon nima vazifani bajaradi ? | \*Obyekt |
| 559 | Foydalanishna boshqarishning nechta usuli  mavjud? | \*4 |
| 560 | Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun  qo‘llaniladi | ABAC |
| 561 | Foydalanishni boshqarishning qaysi modelida  Obyekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi | ABAC |
| 562 | Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni  klassifikatsiyalashga asosan boshqariladi. | ABAC |
| 563 | Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bog‘liq.. | Tashkilotda Obyektning muhimlik darajasi  bilan yoki yuzaga keladigan foyda miqdori bilan bilan xarakterlanadi |
| 564 | MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan  amalga oshiriladi | \*xavfsizlik siyosati ma’muri |
| 565 | Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u  holda uchun qanday amalga ruxsat beriladi | Yozish |
| 566 | Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday  amalga ruxsat beriladi. | \*Yozish |

|  |  |  |
| --- | --- | --- |
| 567 | Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun  Obyektlardan foydalanish ruxsati ko‘rsatiladi? | ABAC |
| 568 | Rol tushunchasiga ta’rif bering. | \*Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida  belgilanishi mumkin |
| 569 | Foydalanishni boshqarishning qaysi usuli - Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish  asosida foydalanishlarni boshqaradi. | \*ABAC |
| 570 | XACML foydalanishni boshqarishni qaysi  usulining standarti? | \*ABAC |
| 571 | Biometrik autentifikatsiyalash usullari an’anaviy  usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan? | \*barchasi |
| 572 | Axborotning kriptografik himoya vositalari necha  turda? | 4 |
| 573 | Dasturiy shifrlash vositalari necha turga bo‘linadi | \*4 |
| 574 | Diskni shifrlash nima uchun amalga oshiriladi? | \*Ma’lumotni saqlash vositalarida saqlangan  ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi |
| 575 | Ma’lumotlarni yo‘q qilish odatda necha hil  usulidan foydalaniladi? | 8 |
| 576 | Kompyuter tarmoqlari bu – | \*Bir biriga osonlik bilan ma’lumot va  resurslarni taqsimlash uchun ulangan kompyuterlar guruhi |
| 577 | Tarmoq modeli –bu.. ikki | Matematik modellar to‘plami |
| 578 | OSI modelida nechta tarmoq satxi bor | \*7 |
| 579 | OSI modeli 7 satxi bu | \*Ilova |
| 580 | OSI modeli 1 satxi bu | Ilova |
| 581 | OSI modeli 2 satxi bu | Ilova |
| 582 | TCP/IP modelida nechta satx mavjud | \*4 |
| 583 | Qanday tarmoq qisqa masofalarda qurilmalar  o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi? | Lokal |
| 584 | Tarmoq kartasi bu... | \*Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash  imkoniyatini taqdim etadi. |
| 585 | Switch bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash  imkoniyatini taqdim etadi. |
| 586 | Hab bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash  imkoniyatini taqdim etadi. |
| 587 | Tarmoq repiteri bu... | Hisoblash qurilmasining ajralmas qismi  bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |

|  |  |  |
| --- | --- | --- |
| 588 | Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini  amalga oshiradi. | \*DNS tizimlari |
| 589 | ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq  ulanishlarini sozlashga yordam beradi. | \*TCP |
| 590 | …. protokolidan odatda o‘yin va video ilovalar  tomonidan keng foydalaniladi. | \*UDP |
| 591 | Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil  ma’lumotlari bilan ta’minlaydi. | TCP |
| 592 | Tarmoq taxdidlari necha turga bo‘linadi | 2 |
| 593 | Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi  axborotni to‘plashni maqsad qiladi; | \*Razvedka hujumlari |
| 594 | Qanday xujum hujumchi turli texnologiyalardan  foydalangan holda tarmoqqa kirishga harakat qiladi | Razvedka hujumlari |
| 595 | Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud  bo‘lgan biror xizmatni cheklashga urinadi; | Razvedka hujumlari |
| 596 | Qanday xujumdp zararli hujumlar tizim yoki  tarmoqqa bevosita va bilvosita ta’sir qiladi; | Razvedka hujumlari |
| 597 | RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart? | \*e soni Eyler funksiyasi -  bilan o‘zaro tub |
| 598 | RSA elektron raqamli imzo algoritmidagi yopiq kalit  d qanday hisoblanadi? Bu yerda p va q tub sonlar,n=pq, - Eyler funksiyasi,e-ochiq  kalit | \* |
| 599 | Elektron raqamli imzo algoritmi qanday  bosqichlardan iborat bo‘ladi? | \*Imzo qo‘yish va imzoni tekshirishdan |
| 600 | Imzoni haqiqiyligini tekshirish qaysi kalit  yordamida amalga oshiriladi? | \*Imzo muallifining ochiq *kaliti yordamida* |
| 601 | **Tarmoq modeli-bu...** | \*Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar  muvaffaqqiyatli o‘rnatilishini asosidir |
| 602 | OSI modeli nechta satxga ajraladi? | 2 |
| 603 | Fizik satxning vazifasi nimadan iborat | \*Qurilma, signal va binar o‘zgartirishlar |
| 604 | Ilova satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
| 605 | Kanal satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
| 606 | Tarmoq satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
| 607 | TCP/IP modeli nechta satxdan iborat | \*4 |
| 608 | Quyidagilarninf qaysi biri Kanal satxi protokollari | \*Ethernet, Token Ring, FDDI, X.25, Frame  Relay, RS-232, v.35. |
| 609 | Quyidagilarninf qaysi biri tarmoq satxi  protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
| 610 | Quyidagilarninf qaysi biri transport satxi  protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |

|  |  |  |
| --- | --- | --- |
| 611 | Quyidagilarninf qaysi biri ilova satxi protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
| 612 | TCP/IP modelining kanal satxiga OSI modelining  qaysi satxlari mos keladi | \*Kanal, Fizik |
| 613 | TCP/IP modelining tarmoq satxiga OSI  modelining qaysi satxlari mos keladi | Kanal, Fizik |
| 614 | TCP/IP modelining transport satxiga OSI  modelining qaysi satxlari mos keladi | Kanal, Fizik |
| 615 | TCP/IP modelining ilova satxiga OSI modelining  qaysi satxlari mos keladi | Kanal, Fizik |
| 616 | Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang. | \*Kompyuterlar va ularni bog‘lab turgan  qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
| 617 | Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta  tarmoqda bo‘ladi. |
| 618 | Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta  tarmoqda bo‘ladi. |
| 619 | Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan  qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
| 620 | Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan | \*Tarmoqda har bir kompyuter yoki tugun  Markaziy tugunga individual bog‘langan bo‘ladi |
| 621 | Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan  bo‘ladi |
| 622 | Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun  markaziy tugunga individual bog‘langan bo‘ladi |
| 623 | Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun  markaziy tugunga individual bog‘langan bo‘ladi |
| 624 | Tarmoq kartasi nima? | \*Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash  imkoniyatini taqdim etadi |
| 625 | Repetir nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash  imkoniyatini taqdim etadi |
| 626 | Hub nima? | Hisoblash qurilmasining ajralmas qismi  bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
| 627 | Switch nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash  imkoniyatini taqdim etadi |
| 628 | Router nima? | Hisoblash qurilmasining ajralmas qismi  bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
| 629 | DNS tizimlari. | \*Host nomlari va internet nomlarini IP  manzillarga o‘zgartirish yoki teskarisini amalga oshiradi |

|  |  |  |
| --- | --- | --- |
| 630 | TCP bu- … | \*Transmission Control Protocol |
| 631 | UDP bu-… | User domain protocol |
| 632 | IP protokolining necha xil versiyasi mavjud? | 1 |
| 633 | Tarmoq xavfsizligiga tahdidlar tavsiflangan  bandni belgilang | \*Ichki, tashqi |
| 634 | Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib  keladi | \*Biznes jarayonlarni to‘xtab qolishiga olib keladi |
| 635 | Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib  keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
| 636 | Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib  keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
| 637 | Tarmoq xavfsizligining buzilishi natijasida  axborotning o’g’irlanishi qanday oqibatlarga olib keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
| 638 | Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi | \*Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya  usullarining yetarlicha bardoshli bo‘lmasligi |
| 639 | Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya  usullarining yetarlicha bardoshli bo‘lmasligi |
| 640 | Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. | Tarmoq qurilmalari, svitch yoki routerlardagi  autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi |
| 641 | Asosan tarmoq, tizim va tashkilot haqidagi  axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi | \*Razvedka hujumlari |
| 642 | Razvedka hujumiga berilgan ta’rifni aniqlang | \*Asosiy hujumlarni oson amalga oshirish  uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
| 643 | Kirish hujumiga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish  uchun tashkilot va tarmoq haqidagi axboro ni to‘plashni maqsad qiladi; |
| 644 | DOS hujumiga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish  uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
| 645 | Zararli hujumga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni  to‘plashni maqsad qiladi; |
| 646 | Razvetka hujumari necha turga bo’linadi | 1 |
| 647 | Qaysi hujum jarayoni TCP/IP tarmog‘ida paketlarni tutib  olish, dekodlash, tekshirish va tarjima qilishni o‘z ichiga  oladi | \*Paketlarni snifferlash |
| 648 | Tarmoqlaro ekranni OSI modeli bo’yicha qanday turlarga bo’lindi? | \*• paket filterlari tarmoq satxida ishlaydi;  ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida |

|  |  |  |
| --- | --- | --- |
| 649 | Tarmoqlaro ekranni foydalanilgan texnologiyasi bo’yicha qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida  ishlaydi; ilova proksilari – ilova satxida |
| 650 | Tarmoqlaro ekranni bajarilishiga ko’ra qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida  ishlaydi; ilova proksilari – ilova satxida |
| 651 | Tarmoqlaro ekranni ulanish sxemasi bo’yicha qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport  sahidaishlaydi; ilova proksilari – ilova satxida |
| 652 | Paket filtrlari tarmoqlararo ekrani vazifasi nima? | \*Tarmoq satxida paketlarni  tahlillashga asoslan; |
| 653 | Ilova proksilari tarmoqlararo ekrani vazifasi  nima? | Tarmoq satxida paketlarni tahlillashga  asoslan; |
| 654 | Ekspert paket filtrlari tarmoqlararo ekrani vazifasi  nima? | Tarmoq satxida paketlarni tahlillashga  asoslan; |
| 655 | Quyidagilardan qaysi biri paket filtrlari tarmoqlararo ekrani kamchiligini ifodalaydi. | \*Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma’lumotlarni,  zararli dasturlarni va hak. tekshirmaydi. |
| 656 | Quyidagilardan qaysi biri ekspert paket filtrlari tarmoqlararo ekrani kamchiligini ifodalaydi. | Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma’lumotlarni, zararli  dasturlarni va hak. tekshirmaydi. |
| 657 | Simsiz tarmoqlarning nechta turi mavjud | 5 |
| 658 | Bluetooth qanday simsiz tarmoq turiga kiradi. | Global |
| 659 | Wifi qanday simsiz tarmoq turiga kiradi. | Global |
| 660 | LTE, CDMA, HSDPA qanday simsiz tarmoq  turiga kiradi. | \*Global |
| 661 | WiMAX qanday simsiz tarmoq turiga kiradi. | Global |
| 662 | Bluetooth texnologiyasida autentifikatsiya bu… | Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash  amalga oshirish. |
| 663 | Bluetooth texnologiyasida konfidensiallik bu… | \*Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan  hujumlardan himoyalash uchun shifrlash amalga oshirish. |
| 664 | Bluetooth texnologiyasida avtorizatsiya bu… | Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan  hujumlardan himoyalash uchun shifrlash amalga oshirish. |
| 665 | GSM bu ..- | \*Global System for Mobile Communications |
| 666 | Simsiz tarmoq Bluetooth ishlash rejimlari nechta? | 2 |
| 667 | Kompyuterda hodisalar haqidagi ma’lumot  qayerda saqlanadi? | \*hodisalar jurnaliga |
| 668 | Windows operatsion tizimida xatolik hodisasiga berilgan ta’rifni belgilang. | \*Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa,  xatolik hodisasi qayd yetiladi. |

|  |  |  |
| --- | --- | --- |
| 669 | Windows operatsion tizimida ogohlantirish hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa,  xatolik hodisasi qayd yetiladi. |
| 670 | Windows operatsion tizimida axborot hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa,  xatolik hodisasi qayd yetiladi. |
| 671 | Windows operatsion tizimida muvaffaqiyatli audit hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat  ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
| 672 | Windows operatsion tizimida muvaffaqiyatsiz audit hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa,  xatolik hodisasi qayd yetiladi. |
| 673 | Ma’lumotlarni zaxira nusxalash bu – … | \*Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot  yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi |
| 674 | Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash  uchun qanday amaldan foydalanamiz | \*Zaxira nusxalash |
| 675 | Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering | \*Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar  bazasini xatolik bilan boshqarilganligi. |
| 676 | Ma’lumotlarni g’arazli hatti harakatlar yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini  to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
| 677 | Ma’lumotlarni tasodifiy sabablar tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar  bazasini xatolik bilan boshqarilganligi. |
| 678 | Ma’lumotlarni tabiiy ofatlar tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar  bazasini xatolik bilan boshqarilganligi. |
| 679 | Zahira nusxalash strategiyasi nechta bosqichni o’z  ichiga oladi? | 7 |
| 680 | Zaxiralash uchun zarur axborotni aniqlash nechta  bosqichda amalga oshiriladi. | \*4 |
| 681 | Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash | \*Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega  bo‘lishi shart. |

|  |  |  |
| --- | --- | --- |
| 682 | Zaxira nusxalovchi vositalar tanlashdagi  *ishonchlilik* xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega  bo‘lishi shart. |
| 683 | Zaxira nusxalovchi vositalar tanlashdagi tezlik xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega  bo‘lishi shart. |
| 684 | Zaxira nusxalovchi vositalar tanlashdagi foydalanuvchanlik xuusiyatiga berilgan ta’rifni  nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega  bo‘lishi shart. |
| 685 | Zaxira nusxalovchi vositalar tanlashdagi qulaylik xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega  bo‘lishi shart. |
| 686 | RAID texnologiyasining transkripsiyasi qanday. | Redundant Array of Independent Disks |
| 687 | RAID texnologiyasida nechta satx mavjud | 3 |
| 688 | RAID 0: diskni navbatlanishi bu-.. | \*Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi.  Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
| 689 | RAID 1: diskni navbatlanishi bu-.. | Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi.  Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
| 690 | RAID 3: diskni navbatlanishi bu-.. | Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi. Agar disk buzilsa, ma’lumotni tiklab  bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
| 691 | RAID 5: diskni navbatlanishi bu-.. | Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi. Agar disk buzilsa, ma’lumotni tiklab  bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
| 692 | RAID 10: diskni navbatlanishi bu-.. | \*Gibrid satx bo‘lib, RAID 1 va RAID 0 satxlaridan iborat va kamida 4 ta diskni talab  etadi |
| 693 | RAID 50: diskni navbatlanishi bu-.. | Gibrid satx bo‘lib, RAID 1 va RAID 0 satxlaridan iborat va kamida 4 ta diskni talab  etadi |
| 694 | Ma’lumotlarni nusxalash usullari necha xil usulda  amalga oshiriladi? | \*3 |
| 695 | Issiq zaxiralash usuliga berilgan ta’rifni belgilang. | \*Ushbu usulda foydalanuvchi tizimni boshqarayotgan  vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.  Mazkur zaxiralash usulini amalga oshirish tizimni |

|  |  |  |
| --- | --- | --- |
|  |  | harakatsiz vaqtini kamaytiradi. |
| 696 | Iliq zaxiralash usuliga berilgan ta’rifni belgilang. | Ushbu usulda foydalanuvchi tizimni boshqarayotgan  vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.  Mazkur zaxiralash usulini amalga oshirish tizimni  harakatsiz vaqtini kamaytiradi. |
| 697 | Sovuq zaxiralash usuliga berilgan ta’rifni belgilang. | Ushbu usulda foydalanuvchi tizimni boshqarayotgan  vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.  Mazkur zaxiralash usulini amalga oshirish tizimni  harakatsiz vaqtini kamaytiradi. |
| 698 | Ichki zahiralash qanday amalga oshiriladi | Ichki zahiralashda mahalliy yoki global  serverlardan foydalaniladi |
| 699 | OSI modelining birinchi satxi qanday nomlanadi | \*Fizik satx |
| 700 | OSI modelining ikkinchi satxi qanday nomlanadi | \*Kanal satxi |
| 701 | OSI modelining uchinchi satxi qanday nomlanadi | \*Tarmoq satxi |
| 702 | OSI modelining oltinchi satxi qanday nomlanadi | \*Taqdimlash satxi |
| 703 | OSI modelining ettinchi satxi qanday nomlanadi | \*Amaliy satx |
| 704 | Elektr signallarini qabul qilish va uzatish  vazifalarini OSI modelining qaysi satxi bajaradi | \*Fizik satx |
| 705 | Keltirilgan protokollarning qaysilari transport  satxi protokollariga mansub | \*TCP,UDP |
| 706 | OSI modelining fizik satxi qanday funktsiyalarni  bajaradi | \*Elektr signallarini uzatish va qabul qilish |
| 707 | OSI modeliningamaliy satxi qanday funktsiyalarni  bajaradi | \*Klient dasturlari bilan o’zaro muloqotda  bo’lish |
| 708 | 12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan  sonlar soni nechta? | 6 ta |
| 709 | Yevklid algoritmi qanday natijani beradi? | \*Sonning eng katta umumiy bo’luvchisini  toppish |
| 710 | Qanday sonlar tub sonlar deb yuritiladi? | \*Faqatgina 1 ga va o’ziga bo’linadigan sonlar  tub sonlar deyiladi. |
| 711 | To‘liq zaxiralash | Tiklashning tezligi yuqori. axira nusxalash  jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi |
| 712 | O‘sib boruvchi zaxiralash | Tiklashning tezligi yuqori. Zaxira nusxalash  jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi |
| 713 | Differnsial zaxiralash | Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma’lumotni saqlash  uchun ko‘p hajm talab etadi |
| 714 | Ushbu jarayon ma’lumot qanday yo‘qolgani, ma’lumotni qayta tiklash dasturiy vositasi va ma’lumotni tiklash anzilini qayergaligiga bog‘liq  bo‘ladi. Qaysi jarayon | Ma’lumotlarni qayta tiklash |
| 715 | Antivirus dasturlarini ko’rsating? | \*Drweb, Nod32, Kaspersky |

|  |  |  |
| --- | --- | --- |
| 716 | Wi-Fi tarmoqlarida quyida keltirilgan qaysi  shifrlash protokollaridan foydalaniladi | \*wep, wpa, wpa2 |
| 717 | Axborot himoyalangan qanday sifatlarga ega  bo’lishi kerak? | \*ishonchli, qimmatli va to’liq |
| 718 | Axborotning eng kichik o’lchov birligi nima? | \*bit |
| 719 | Virtual xususiy tarmoq – bu? | \*VPN |
| 720 | Xavfli viruslar bu - … | \*kompyuter ishlashida jiddiy nuqsonlarga  sabab bo’luvchi viruslar |
| 721 | Mantiqiy bomba – bu … | \*Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning  alohida modullari |
| 722 | Rezident virus... | \*tezkor xotirada saqlanadi |
| 723 | DIR viruslari nimani zararlaydi? | \*FAT tarkibini zararlaydi |
| 724 | .... kompyuter tarmoqlari bo’yicha tarqalib, kompyuterning tarmoqdagi manzilini aniqlaydi va  u yerda o’zining nusxasini qoldiradi | \*«Chuvalchang» va replikatorli virus |
| 725 | Mutant virus... | \*shifrlash va deshifrlash algoritmlaridan  iborat |
| 726 | Fire Wall ning vazifasi... | \*tarmoqlar orasida aloqa o’rnatish jarayonida  tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi |
| 727 | Kompyuter virusi nima? | \*maxsus yozilgan va zararli dastur |
| 728 | Kompyuterning viruslar bilan zararlanish  yo’llarini ko’rsating | \*disk, maxsus tashuvchi qurilma va  kompyuter tarmoqlari orqali |
| 729 | Troyan dasturlari bu... | \*virus dasturlar |
| 730 | Kompyuter viruslari xarakterlariga nisbatan necha  turga ajraladi? | \*5 |
| 731 | Antiviruslarni, qo’llanish usuliga ko’ra... turlari  mavjud | \*detektorlar, faglar, vaktsinalar, privivkalar,  revizorlar, monitorlar |
| 732 | Axborotni himoyalash uchun ... usullari  qo’llaniladi. | \*kodlashtirish, kriptografiya, stegonografiya |
| 733 | Stenografiya mahnosi... | \*sirli yozuv |
| 734 | …sirli yozuvning umumiy nazariyasini yaratdiki,  u fan sifatida stenografiyaning bazasi hisoblanadi | \*K.Shennon |
| 735 | Kriptologiya yo’nalishlari nechta? | \*2 |
| 736 | Kriptografiyaning asosiy maqsadi... | \*maxfiylik, yaxlitlilikni ta`minlash |
| 737 | Zararli dasturiy vositalarni aniqlash turlari nechta | \*3 |
| 738 | Signaiurana asoslangan | \* bu fayldan topilgan bitlar qatori bo‘lib,  maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh  qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
| 739 | O‘zgarishni aniqlashga asoslangan | ....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh  qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
| 740 | Anomaliyaga asoslangan | ....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda  ularning xesh |

|  |  |  |
| --- | --- | --- |
|  |  | qiymatlari ham signatura sifatida xizmat  qilishi mumkin. |
| 741 | Antiairuslar qanday usulda viruslarni aniqlaydi | Anomaliyaga asoslangan |
| 742 | Viruslar - | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat  bo‘ladi |
| 743 | Rootkitlar- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat  bo‘ladi |
| 744 | Backdoorlar - | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vositasifatida ko‘rinsada,  yashiringan zararli koddan iborat bo‘ladi |
| 745 | Troyan otlari- | \*bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida  ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
| 746 | Ransomware- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat  bo‘ladi |
| 747 | Resurslardan foydalanish usuliga ko’ra viruslar  qanday turlarga bo’linadi | \*Virus parazit, Virus cherv |
| 748 | Zararlagan obyektlar turiga ko’ra | Virus parazit, Virus cherv |
| 749 | Faollashish prinspiga ko’ra | Virus parazit, Virus cherv |
| 750 | Dastur kodini tashkil qilish yondashuviga ko‘ra | Virus parazit, Virus cherv |
| 751 | Shifrlanmagan viruslar | \*o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha  ishlashlar mavjud bo‘lmaydi. |
| 752 | Shifrlangan viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha  ishlashlar mavjud bo‘lmaydi. |
| 753 | Polimorf viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va  bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
| 754 | Dasturiy viruslar-… | bir vaqtning o‘zida turli xildagi Obyektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word  hujjatlarini ham zararlay oladi. |
| 755 | Ko‘p platformali viruslar | \*bir vaqtning o‘zida turli xildagi Obyektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va  Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. |
| 756 | Yuklanuvchi viruslar | bir vaqtning o‘zida turli xildagi Obyektlarni |

|  |  |  |
| --- | --- | --- |
|  |  | zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word  hujjatlarini ham zararlay oladi. |
| 757 | Makroviruslar-... | bir vaqtning o‘zida turli xildagi Obyektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word  hujjatlarini ham zararlay oladi. |
| 758 | Birinchi kompyuter virusi nima deb nomlangan | Cherv |
| 759 | P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang | \*840 |
| 760 | 256mod25=? | 5 |
| 761 | bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima  deyiladi. | \*Tizim |
| 762 | Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori satxli hujjat yoki hujjatlar to‘plami nima  duyidadi | Standart |
| 763 | RSA shifrlash algoritmida foydalaniladigan  sonlarning spektori o‘lchami qanday? | 65535; |
| 764 | DES algoritmi akslantirishlari raundlari soni  qancha? | \*16; |
| 765 | DES algoritmi shifrlash blokining chap va o‘ng  qism bloklarining o‘lchami qancha? | CHap qism blok 32 bit, o‘ng qism blok 48 bit; |
| 766 | Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli  tomonlari bor? | SHifrlash va deshifrlash jarayonlarida kalitlardan foydalanish qoidalariga ko‘ra  farqlanadi |
| 767 | 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan  sonlar soni nechta? | 19 ta |
| 768 | 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan  sonlar soni nechta? | \*4 ta |
| 769 | Qaysi formula qoldiqli bo’lish qonunini  ifodalaydi |  |
| 770 | Eyler funsiyasida 𝜙(1) qiymati nimaga teng? | \*0 |
| 771 | Eyler funksiyasida 60 sonining qiymatini toping. | 59 |
| 772 | Eyler funksiyasi yordamida 1811 sonining  qiymatini toping. | \*1810 |
| 773 | 97 tub sonmi? | \*Tub |
| 774 | Quyidagi modulli ifodani qiymatini toping  (148 + 14432) mod 256. | \*244 |
| 775 | Quyidagi sonlarning eng katta umumiy  bo’luvchilarini toping. 88 i 220 | 21 |
| 776 | Quyidagi ifodani qiymatini toping.  -17mod11 | 6 |
| 777 | 2 soniga 10 modul bo’yicha teskari sonni toping. | 3 |

### 778. I:

779. S: Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.

780. +: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik

1. -: Axborot va Iqtisodiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xafvsizligi, Dasturiy ta`minot xavfsizligi
2. -: Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xafvsizligi, Ekologik xavfsizlik
3. -: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Dasturiy ta`minot xavfsizligi, Ekologik xavfsizlik

### I:

1. S: Axborot xavfsizligining asosiy maqsadlaridan biri- bu…

786. +: Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish

1. -:Ob`yektga bevosita ta`sir qilish
2. -: Axborotlarni shifrlash, saqlash, yetkazib berish
3. -: Tarmoqdagi foydalanuvchilarni xavfsizligini ta`minlab berish

### I:

1. S: Konfidentsiallikga to’g’ri ta`rif keltiring.

792. +: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

1. -:axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati;
2. -:axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati;
3. -:axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati;

### I:

1. S: Yaxlitlikni buzilishi bu - …

798. +: Soxtalashtirish va o’zgartirish

1. -: Ishonchsizlik va soxtalashtirish
2. -: Soxtalashtirish
3. -: Butunmaslik va yaxlitlanmaganlik

### I:

1. S:... axborotni himoyalash tizimi deyiladi.

804. +: Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi

1. -: Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo’qotilishidan keladigan zarar va himoyalash mexanizmining narxidan kelib chiqqan holda axborotni himoyalashning zaruriy darajasi
2. -: Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo’qotilishidan keladigan zarar va himoyalash mexanizmining zaruriy darajasi hamda tizimning turini, himoyalash usullar va vositalari
3. -: Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul

### I:

1. S: Kompyuter virusi nima?

810. +: maxsus yozilgan va zararli dastur

1. -:.exe fayl
2. -: boshqariluvchi dastur
3. -: Kengaytmaga ega bo’lgan fayl

### I:

1. S: Kriptografiyaning asosiy maqsadi...

816. +: maxfiylik, yaxlitlilikni ta`minlash

1. -:ishonchlilik, butunlilikni ta`minlash
2. -:autentifikatsiya, identifikatsiya
3. -:ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya

### I:

1. S: SMTP - Simple Mail Transfer protokol nima?

822. +: elektron pochta protokoli

1. -:transport protokoli
2. -:internet protokoli
3. -:Internetda ommaviy tus olgan dastur

### I:

1. S: SKIP protokoli...

828. +: Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi

1. -:Protokollar boshqaruvi
2. -:E-mail protokoli
3. -:Lokal tarmoq protokollari uchun kriptokalitlarning oddiy boshqaruvi

### I:

1. S: Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf- xatarlar…

834. +: uzilish, tutib qolish, o’zgartirish, soxtalashtirish

1. -:o’zgartirish, soxtalashtirish
2. -:tutib qolish, o’zgarish, uzilish
3. -:soxtalashtirish, uzilish, o’zgartirish

### I:

1. S: ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.

840. +: konfidentsiallik

1. -:identifikatsiya
2. -:autentifikatsiya
3. -: maxfiylik

### I:

1. S: Foydalanish huquqini cheklovchi matritsa modeli bu...

846. +: Bella La-Padulla modeli

1. -:Dening modeli
2. -:Landver modeli
3. -:Huquqlarni cheklovchi model

### I:

1. S: Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi?

|  |  |
| --- | --- |
| 852. | +: TCP/IP, X.25 protokollar |
| 853. | -:X.25 protokollar |
| 854. | -:TCP/IP |
| 855. | -:SMTP |
| 856. | I: |

857. S: Autentifikatsiya nima?

858. +: Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi

1. -: Tizim meyoriy va g’ayritabiiy hollarda rejalashtirilgandek o’zini tutishligi holati
2. -: Istalgan vaqtda dastur majmuasining mumkinligini kafolati
3. -:Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi

### I:

1. S:Identifikatsiya bu- …

864. +: Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni

1. -:Ishonchliligini tarqalishi mumkin emasligi kafolati
2. -:Axborot boshlang’ich ko’rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o’zgarishlar
3. -:Axborotni butunligini saqlab qolgan holda uni elementlarini o’zgartirishga yo’l qo’ymaslik

### I:

1. S:O’rin almashtirish shifri bu - …

870. +: Murakkab bo’lmagan kriptografik akslantirish

1. -:Kalit asosida generatsiya qilish
2. -:Ketma-ket ochiq matnni ustiga qo’yish
3. -:Belgilangan biror uzunliklarga bo’lib chiqib shifrlash

### I:

1. S:Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.

876. +: 2 turga

1. -:3 turga
2. -:4 turga
3. -: 5 turga

### I:

1. S: Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular …

882. +: hosil qilish, yig’ish, taqsimlash

1. -:ishonchliligi, maxfiyligi, aniqligi
2. -:xavfsizlik, tez ishlashi, to’g’ri taqsimlanishi
3. -:abonentlar soni, xavfsizligi, maxfiyligi

### I:

1. S: Kriptologiya -

888. +: axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi

1. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
2. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
3. -:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

### I:

1. S: Kriptografiyada alifbo –

894. +: axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam

1. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
2. -:xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
3. -:kalit axborotni shifrlovchi kalitlar

### I:

1. S: Simmetrik kriptotizimlarda ... jumlani davom ettiring

900. +: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi

1. -:bir-biriga matematik usullar bilan bog’langan ochiq va yopiq kalitlardan foydalaniladi
2. -:axborot ochiq kalit yordamida shifrlanadi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi
3. -:kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi

### I:

1. S: Kriptobardoshlilik deb …

906. +: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

1. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
2. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
3. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

### I:

1. S: Elektron raqamli imzo deb –

912. +: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha

1. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
2. -:axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
3. -:kalit axborotni shifrlovchi kalitlar

### I:

1. S: Kriptografiya –

918. +: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

1. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
2. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
3. -:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

### I:

1. S: Kriptografiyada matn –

924. +: alifbo elementlarining tartiblangan to’plami

1. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
2. -:axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
3. -:kalit axborotni shifrlovchi kalitlar

### I:

1. S: Kriptoanaliz –

930. +: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

1. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
2. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
3. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi

### I:

1. S: Shifrlash –

936. +: akslantirish jarayoni ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi

1. -:kalit asosida shifrmatn ochiq matnga akslantiriladi
2. -:shifrlashga teskari jarayon
3. -:Almashtirish jarayoni bo’lib: ochiq matn deb nomlanadigan matn o’girilgan holatga almashtiriladi

### I:

1. S: Faol hujum turi deb…

942. +: Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon

1. -:Maxfiy ma`lumotni aloqa tarmog’ida uzatilayotganda eshitish, tahrir qilish, yozib olish harakatlaridan iborat uzatilalayotgan ma`lumotni qabul qiluvchiga o’zgartirishsiz yetkazish jarayoni
2. -:Ma`lumotga o’zgartirish kiritmay uni kuzatish jarayoni
3. -:Sust hujumdan farq qilmaydigan jarayon

### I:

1. S: Blokli shifrlash-

948. +: shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish

1. -:murakkab bo’lmagan kriptografik akslantirish
2. -:axborot simvollarini boshqa alfavit simvollari bilan almashtirish
3. -:ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi

### I:

1. S: Simmetrik kriptotizmning uzluksiz tizimida …

954. +: ochiq matnning har bir harfi va simvoli alohida shifrlanadi

1. -:belgilangan biror uzunliklarga teng bo’linib chiqib shifrlanadi
2. -:murakkab bo’lmagan kriptografik akslantirish orqali shifrlanadi
3. -:ketma-ket ochiq matnlarni o’rniga qo’yish orqali shifrlanadi

### I:

1. S: Kriptotizimga qo’yiladigan umumiy talablardan biri

960. +: shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak

1. -:shifrlash algoritmining tarkibiy elementlarini o’zgartirish imkoniyati bo’lishi lozim
2. -:ketma-ket qo’llaniladigan kalitlar o’rtasida oddiy va oson bog’liqlik bo’lishi kerak
3. -:maxfiylik o’ta yuqori darajada bo’lmoqligi lozim

### I:

1. S: Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?

966. +: Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

1. -:Asimmetrik tizimlarda k1=k2 bo’ladi, yahni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi
2. -:Asimmetrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma`lum bo’ladi, ochiq kalitni esa faqat qabul qiluvchi biladi
3. -:Asimmetrik kriptotizimlarda k1≠k2 bo’lib, kalitlar hammaga oshkor etiladi

### I:

1. S: Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang

972. +: Vijener matritsasi, Sezar usuli

1. -:monoalfavitli almashtirish
2. -:polialfavitli almashtirish
3. -:o’rin almashtirish

### I:

1. S: Akslantirish tushunchasi deb nimaga aytiladi?

978. +: 1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga

1. -:1-to’plamli elementlariga 2-to’plam elementalrini qarama-qarshiligiga
2. -:har bir elementni o’ziga ko’payimasiga
3. -:agar birinchi va ikinchi to’plam bir qiymatga ega bulmasa

### I:

1. S: Simmetrik guruh deb nimaga aytiladi?

984. +: O’rin almashtirish va joylashtirish

1. -:O’rin almashtirish va solishtirish
2. -:Joylashtirish va solishtirish
3. -:O’rin almashtirish va transportizatsiyalash

### I:

1. S: Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?

990. +: simmetrik kriptosistemalar

1. -:assimetrik kriptosistemalar
2. -:ochiq kalitli kriptosistemalar
3. -:autentifikatsiyalash

### I:

1. S: Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?

996. +: SMTP, POP yoki IMAP

### 997. -:SKIP, ATM, FDDI

998. -:X.25 va IMAR

### 999. -:SMTP, TCP/IP

1000. I:

1001. S: Axborot resursi – bu?

1002. +: axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi

1003. -:cheklanmagan doiradagi shaxslar uchun mo’ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar

1004. -:identifikatsiya qilish imkonini beruvchi rekvizitlari qo’yilgan holda moddiy jismda qayd etilgan axborot

1005. -:manbalari va taqdim etilish shaklidan qathi nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to’g’risidagi ma`lumotlar

### 1006. I:

1007. S: Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya

tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu?

1008. +: login parol 1009. -:identifikatsiya

1010. -:maxfiy maydon

1011. -: token

### 1012. I:

1013. S: Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu?

1014. +: parol

1015. -:login

1016. -:identifikatsiya

1017. -:maxfiy maydon foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni

### 1018. I:

1019. S: Identifikatsiya jarayoni qanday jarayon?

1020. +: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni

1021. -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash

1022. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

1023. -:foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni

### 1024. I:

1025. S: Autentifikatsiya jarayoni qanday jarayon?

1026. +: obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash

1027. -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni

1028. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

1029. -:foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni

### 1030. I:

1031. S: Ro’yxatdan o’tish bu?

1032. +: foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni

1033. -:axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni

1034. -:ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash

1035. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

|  |  |
| --- | --- |
| 1036. | I: |
| 1037. | S: Axborot qanday sifatlarga ega bo’lishi kerak? |
| 1038. | +: ishonchli, qimmatli va to’liq |
| 1039. | -:uzluksiz va uzlukli |

|  |  |
| --- | --- |
| 1040. | -:ishonchli, qimmatli va uzlukli |
| 1041. | -:ishonchli, qimmatli va uzluksiz |
| 1042. | I: |
| 1043. | S: Axborotning eng kichik o’lchov birligi nima? |
| 1044. | +: bit |
| 1045. | -:kilobayt |
| 1046. | -:bayt |
| 1047. | -:bitta simvol |
| 1048. | I: |
| 1049. | S: Elektron hujjatning rekvizitlari nechta qismdan iborat? |
| 1050. | +: 4 |
| 1051. | -:5 |
| 1052. | -:6 |
| 1053. | -:7 |
| 1054. | I: |
| 1055. | S: Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? |
| 1056. | +: fleshka, CD va DVD disklar |
| 1057. | -:Qattiq disklar va CDROM |
| 1058. | -:CD va DVD, DVDROM |
| 1059. | -:Qattiq disklar va DVDROM |
| 1060. | I: |
| 1061. | S: Avtorizatsiya jarayoni qanday jarayon? |
| 1062. | +: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini |

tekshirish jarayoni

1063. -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va -berilgan nom bo’yicha solishtirib uni aniqlash jarayoni

1064. -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash.

1065. -: parollash jarayoni 1066. I:

1067. S: Kodlash nima?

1068. +: Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

1069. -:Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi

1070. mumkin bo‘ladi

1071. -:Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi

1072. mumkin bo‘ladi

1073. -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi

### 1074. I:

1075. S: Shifrlash nima?

1076. +: Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi

1077. -:Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

1078. -: Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi

1079. -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi

### 1080. I:

1081. S: Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi 1082. +:Kriptoanaliz

1083. -:Kartografiya

1084. -:Kriptologiya

1085. -:Adamar usuli

### 1086. I:

1087. S: Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi 1088. +: {d, n} – yopiq, {e, n} – ochiq;

1089. -:{d, e} – ochiq, {e, n} – yopiq;

1090. -:{e, n} – yopiq, {d, n} – ochiq;

1091. -:{e, n} – ochiq, {d, n} – yopiq; 1092. I:

1093. S: Zamonaviy kriptografiya qanday bo’limlardan iborat? 1094. -:Electron raqamli imzo; kalitlarni boshqarish

1095. -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

1096. +: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish

1097. -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; kalitlarni boshqarish 1098. I:

1099. S: Shifr nima?

1100. +: Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm

1101. -:Kalitlarni taqsimlash usuli 1102. -:Kalitlarni boshqarish usuli

1103. -:Kalitlarni generatsiya qilish usuli 1104. I:

1105. S: Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

1106. +: Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

1107. -:Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi

1108. -:Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin 1109. -:Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat deshifrlash mumkin 1110. I:

1111. S: Oqimli shifrlashning mohiyati nimada?

1112. +: Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,

1113. -:Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur,

1114. -:Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi

1115. -:Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,

### 1116. I:

1117. S: Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating. 1118. +: uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi

uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim,

1119. -:uzatilayotgan xabarni xavfsizligi kalitni maxfiyligiga emas, balki algoritmni maxfiyligiga bog’liq bo’lishi lozim

1120. -:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog’liq bo’lishi lozim

1121. -:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga emas, balki shifrlashda foydalaniladigan arifmetik amallar soniga bog’liq bo’lishi lozim

### 1122. I:

1123. S: Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?

1124. +: shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun

1125. -:ERI yaratish va tekshirish, kalitlar almashish uchun 1126. -:shifrlash, deshifrlash, kalitlar almashish uchun 1127. -: Heshlash uchun

### 1128. I:

1129. S: Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi.

1130. +: ochiq kalitlar 1131. -:yopiq kalitlar

1132. -:seans kalitlari

1133. -:Barcha tutdagi kalitlar 1134. I:

1135. S: Kompyuterning tashqi interfeysi deganda nima tushuniladi? 1136. +: kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali

axborot almashinish qoidalari to’plamlari

1137. -:tashqi qurilmani kompyuterga bog’lashda ishlatiladigan ulovchi simlar 1138. -:kompyuterning tashqi portlari.

1139. -:tashqi qurilma bilan kompyuter o’rtasida axborot almashinish qoidalari to’plami

### 1140. I:

1141. S: Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? 1142. +: Yulduz

1143. -:Xalqa

1144. -:To’liqbog’langan

1145. -:Umumiy shina

### 1146. I:

1147. S: Ethernet kontsentratori qanday vazifani bajaradi

1148. +: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi

1149. -:kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo’naltirib beradi

1150. -:kompyuterdan kelayotgan axborotni xalqa bo’ylab joylashgan keyingi kompyuterga

|  |  |
| --- | --- |
| 1151. | -:tarmoqning ikki segmentini bir biriga ulaydi |
| 1152. | I: |
| 1153. | S: OSI modelida nechta satx mavjud |
| 1154. | +: 7 |
| 1155. | -:4 |
| 1156. | -:5 |
| 1157. | -:3 |
| 1158. | I: |
| 1159. | S: OSI modelining to’rtinchi satxi qanday nomlanadi |
| 1160. | +: Transport satxi |
| 1161. | -:Amaliy satx |
| 1162. | -:Seanslar satxi |
| 1163. | -:Taqdimlash satxi |
| 1164. | I: |
| 1165. | S: OSI modelining beshinchi satxi qanday nomlanadi |
| 1166. | +: Seanslar satxi |
| 1167. | -:Tarmoq satxi |
| 1168. | -:Fizik satx |
| 1169. | -:Amaliy satx |
| 1170. | I: |
| 1171. | S: OSI modelining birinchi satxi qanday nomlanadi |
| 1172. | +: Fizik satx |
| 1173. | -:Seanslar satxi |
| 1174. | -:Transport satxi |
| 1175. | -:Taqdimlash satxi |
| 1176. | I: |
| 1177. | S: OSI modelining ikkinchi satxi qanday nomlanadi |
| 1178. | +: Kanal satxi |
| 1179. | -:Amaliy satxi |
| 1180. | -:Fizik satx |
| 1181. | -:Seanslar satxi |
| 1182. | I: |
| 1183. | S: OSI modelining uchinchi satxi qanday nomlanadi |
| 1184. | +: Tarmoq satxi |
| 1185. | -:Amaliy satx |
| 1186. | -:Kanal satxi |
| 1187. | -:Taqdimlash satxi |
| 1188. | I: |
| 1189. | S: OSI modelining oltinchi satxi qanday nomlanadi |
| 1190. | +: Taqdimlash satxi |
| 1191. | -:Amaliy satx |
| 1192. | -:Seanslar satxi |
| 1193. | -:Kanal satxi |
| 1194. | I: |
| 1195. | S: OSI modelining yettinchi satxi qanday nomlanadi |
| 1196. | +: Amaliy satx |
| 1197. | -:Seanslar satxi |
| 1198. | -:Transport satxi |

|  |  |
| --- | --- |
| 1199. | -:Taqdimlash satxi |
| 1200. | I: |
| 1201. | S: OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi |
| 1202. | +: fizik, kanal va tarmoq satxlari |
| 1203. | -:seans va amaliy satxlar |
| 1204. | -:amaliy va taqdimlash satxlari |
| 1205. | -:transport va seans satxlari |
| 1206. | I: |
| 1207. | S: OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi |
| birida bajariladi | |
| 1208. | +: Marshrutizator |
| 1209. | -:Ko’prik |
| 1210. | -:Tarmoq adapter |
| 1211. | -:Kontsentrator |
| 1212. | I: |
| 1213. | S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining |
| qaysi satxi bajaradi | |
| 1214. | +: Fizik satx |
| 1215. | -:Kanal satxi |
| 1216. | -:Tarmoq satxi |
| 1217. | -:Transport satxi |
| 1218. | I: |
| 1219. | S: Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini |
| OSI modelining qaysi satxi bajaradi | |
| 1220. | +: Tarmoq satxi |
| 1221. | -:Kanal satxi |
| 1222. | -:Amaliy satx |
| 1223. | -:Transport satxi |
| 1224. | I: |
| 1225. | S: Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub |
| 1226. | +: IP, IPX |
| 1227. | -:NFS, FTP |
| 1228. | -:Ethernet, FDDI |
| 1229. | -:TCP,UDP |
| 1230. | I: |
| 1231. | S: Keltirilgan protokollarning qaysilari transport satxi protokollariga |
| mansub | |
| 1232. | +: TCP,UDP |
| 1233. | -:NFS, FTP |
| 1234. | -:IP, IPX |
| 1235. | -:Ethernet, FDDI |
| 1236. | I: |
| 1237. | S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi |
| 1238. | +: Elektr signallarini uzatish va qabul qilish |
| 1239. | -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojaat qilishni |

boshqarish

1240. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash 1241. -:Klient dasturlari bilan o’zaro muloqotda bo’lish

### 1242. I:

1243. S: Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...

|  |  |
| --- | --- |
| 1244. | +: Avtorizatsiya |
| 1245. | -:Shifrlash |
| 1246. | -:Identifikatsiya |
| 1247. | -:Autentifikatsiya |
| 1248. | I: |
| 1249. | S: Autentifikatsiya faktorlari nechta |
| 1250. | +: 3 |
| 1251. | -:4 |
| 1252. | -:5 |
| 1253. | -: 6 |
| 1254. | I: |
| 1255. | S: Ko‘z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi |
| faktoriga mos belgilar? | |
| 1256. | +: Biometrik autentifikatsiya |
| 1257. | -:Biron nimaga egalik asosida |
| 1258. | -:Biron nimani bilish asosida |
| 1259. | -:Parolga asoslangan |
| 1260. | I: |
| 1261. | S: Barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; |
| tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi? | |
| 1262. | +: Fizik satx |
| 1263. | -:Tarmoq satxi |
| 1264. | -:Amaliy satx |
| 1265. | -:Tadbiqiy sath |
| 1266. | I: |
| 1267. | S: Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi |
| 1268. | +: 2 |
| 1269. | -:4 |
| 1270. | -:3 |
| 1271. | -:5 |
| 1272. | I: |
| 1273. | S: Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima |
| vazifani bajaradi? | |
| 1274. | +: Subyekt |
| 1275. | -:Obyekt |
| 1276. | -:Tizim |
| 1277. | -:Jarayon |
| 1278. | I: |
| 1279. | S: MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan |
| holatda kim tomonidan amalga oshiriladi | |
| 1280. | +: xavfsizlik siyosati ma’muri |
| 1281. | -:Foydalaguvchining o‘zi |
| 1282. | -:Dastur tomonidan |
| 1283. | -:Boshqarish amaalga oshirilmaydi |

### 1284. I:

1285. S: Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi

1286. +: O‘qish

1287. -:Yozish

1288. -:O‘zgartirish

1289. -:Yashirish

### 1290. I:

1291. S: Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.

1292. +: Yozish

1293. -:O‘qish

1294. -:O‘zgartirish

1295. -:Yashirish

### 1296. I:

1297. S: Rol tushunchasiga ta’rif bering.

1298. +: Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin

1299. -:Foydalanishni boshqarish

1300. -:Muayyan faoliyat turi bilan bog‘liq imkoniyatlar to‘plami sifatida belgilanishi mumkin

|  |  |
| --- | --- |
| 1301. | -:Vakolitlarni taqsimlash |
| 1302. | I: |
| 1303. | S: Foydalanishni boshqarishning qaysi usuli - Obyektlar va Subyektlarning |
| atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. | |
| 1304. | +: ABAC |
| 1305. | -:MAC |
| 1306. | -:DAC |
| 1307. | -:RBAC |
| 1308. | I: |
| 1309. | S: Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan |
| avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan? | |
| 1310. | +: barchasi |
| 1311. | -:bimetrik alomatlarning ishga layoqatli shaxsdan ajratib bo‘lmasligi |
| 1312. | -:biometrik alomatlarni soxtalashtirishning qiyinligi |
| 1313. | -:biometrik alomatlarni noyobligi tufayli autentifikatsiyalashning |
| ishonchlilik darajasi yuqoriligi | |
| 1314. | I: |
| 1315. | S: OSI modeli 7 satxi bu |
| 1316. | +: Ilova |
| 1317. | -:Seans |
| 1318. | -:Fizik |
| 1319. | -:Kanal |
| 1320. | I: |
| 1321. | S: OSI modeli 1 satxi bu |
| 1322. | +: Fizik |
| 1323. | -:Ilova |

|  |  |
| --- | --- |
| 1324. | -:Seans |
| 1325. | -:Kanal |
| 1326. | I: |
| 1327. | S: OSI modeli 2 satxi bu |
| 1328. | +:Kanal |
| 1329. | -: Fizik |
| 1330. | -:Ilova |
| 1331. | -:Seans |
| 1332. | I: |
| 1333. | S: TCP/IP modelida nechta satx mavjud |
| 1334. | +: 4 |
| 1335. | -:3 |
| 1336. | -:2 |
| 1337. | -:8 |
| 1338. | I: |
| 1339. | S: Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot |
| almashinish imkoniyatini taqdim etadi? | |
| 1340. | +: Shaxsiy tarmoq |
| 1341. | -:Lokal |
| 1342. | -:Mintaqaviy |
| 1343. | -:CAMPUS |
| 1344. | I: |
| 1345. | S: Tarmoq kartasi bu... |
| 1346. | +: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash |

imkoniyatini taqdim etadi.

1347. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.

1348. -:ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.

1349. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.

### 1350. I:

1351. S: Server xotirasidagi joyni bepul yoki pulli ijagara berish xizmati qanday ataladi?

1352. +: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.

1353. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

1354. -:Signalni tiklash yoki qaytarish uchun foydalaniladi.

1355. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.

### 1356. I:

1357. S: Hab bu...

1358. +: ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.

1359. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

1360. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.

1361. -:qabul qilingan signalni barchachiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.

### 1362. I:

1363. S: Tarmoq repiteri bu...

1364. +: Signalni tiklash yoki qaytarish uchun foydalaniladi.

1365. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

1366. -:ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.

1367. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.

### 1368. I:

1369. S: Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi.

1370. +: DNS tizimlari 1371. -:TCP/IP

1372. -:Ethernet

1373. -:Token ring

### 1374. I:

1375. S: ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.

|  |  |
| --- | --- |
| 1376. | +: TCP |
| 1377. | -:IP |
| 1378. | -:HTTP |
| 1379. | -:FTP |
| 1380. | I: |
| 1381. | S: …. protokolidan odatda o‘yin va video ilovalar tomonidan keng |
| foydalaniladi. | |
| 1382. | +: UDP |
| 1383. | -:HTTP |
| 1384. | -:TCP |
| 1385. | -:FTP |
| 1386. | I: |
| 1387. | S: Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun |
| zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi. | |
| 1388. | +: IP |
| 1389. | -:TCP |
| 1390. | -:HTTP |
| 1391. | -:FTP |
| 1392. | I: |
| 1393. | S: Tarmoq taxdidlari necha turga bo‘linadi |
| 1394. | +: 4 |
| 1395. | -:2 |
| 1396. | -:3 |
| 1397. | -:5 |

### 1398. I:

|  |  |
| --- | --- |
| 1400. | +: Razvedka hujumlari |
| 1401. | -:Kirish hujumlari |
| 1402. | -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari |
| 1403. | -:Zararli hujumlar |
| 1404. | I: |
| 1405. | S: Qanday xujum hujumchi turli texnologiyalardan foydalangan holda |
| tarmoqqa kirishga harakat qiladi | |
| 1406. | +: Kirish hujumlari |
| 1407. | -:Razvedka hujumlari |
| 1408. | -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari |
| 1409. | -:Zararli hujumlar |
| 1410. | I: |
| 1411. | S: Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va |
| tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi; | |
| 1412. | +: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari |
| 1413. | -:Razvedka hujumlari |
| 1414. | -:Kirish hujumlari |
| 1415. | -:Zararli hujumlar |
| 1416. | I: |
| 1417. | S: Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va |
| bilvosita ta’sir qiladi; | |
| 1418. | +: Zararli hujumlar |
| 1419. | -:Razvedka hujumlari |
| 1420. | -:Kirish hujumlari |
| 1421. | -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari |
| 1422. | I: |
| 1423. | S: RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni |
| qanoatlantirishi shart? | |
| 1424. | +: e soni Eyler funksiyasi - 𝜑(𝑛) bilan o‘zaro tub |
| 1425. | -:e ning qiymati [1,n] kesmaga tegishli ixtiyoriy son |
| 1426. | -:e soni ixtiyoriy tub son |
| 1427. | -:e soni ixtiyoriy butun musbat son |
| 1428. | I: |
| 1429. | S: RSA elektron raqamli imzo algoritmidagi yopiq kalit d qanday |
| hisoblanadi? Bu yerda p va q tub sonlar,n=pq, 𝜑(𝑛)- Eyler funksiyasi,e-ochiq ka 1430. +: 𝑑 = 𝑒−1𝑚𝑜𝑑𝜑(𝑛) | |
| 1431. | -: 𝑑 = 𝑒−1𝑚𝑜𝑑𝑞 |
| 1432. | -:𝑑 = 𝑒−1𝑚𝑜𝑑𝑞 |
| 1433. | -:𝑑 = 𝑒−1𝑚𝑜𝑑𝑝 |
| 1434. | I: |
| 1435. | S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? |
| 1436. | +: Imzo qo‘yish va imzoni tekshirishdan |
| 1437. | -:Faqat imzo qo‘yishdan |
| 1438. | -:Faqat imzoni tekshirishdan |

1399. S: Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;

lit

|  |  |
| --- | --- |
| 1439. | -:Barcha javoblar to‘g‘ri |
| 1440. | I: |
| 1441. | S: Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? |
| 1442. | +: Imzo muallifining ochiq kaliti yordamida |
| 1443. | -:Ma’lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida |
| 1444. | -:Ma’lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida |
| 1445. | -:Imzo muallifining maxfiy kaliti yordamida |
| 1446. | I: |
| 1447. | S: Tarmoq modeli-bu... |
| 1448. | +: Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va |
| texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir | |
| 1449. | -:Global tarmoq qurish usullari |
| 1450. | -:Lokal tarmoq qurish usullari |
| 1451. | -:To‘g‘ri javob yo‘q. |
| 1452. | I: |
| 1453. | S: OSI modeli nechta satxga ajraladi? |
| 1454. | +: 7 |
| 1455. | -:2 |
| 1456. | -:4 |
| 1457. | -:3 |
| 1458. | I: |
| 1459. | S: TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos |
| keladi | |
| 1460. | +: Kanal, Fizik |
| 1461. | -:Tarmoq |
| 1462. | -:Tramsport |
| 1463. | -:Ilova, taqdimot, seans. |
| 1464. | I: |
| 1465. | S: TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos |
| keladi | |
| 1466. | +: Tarmoq |
| 1467. | -:Kanal, Fizik |
| 1468. | -:Tramsport |
| 1469. | -:Ilova, taqdimot, seans. |
| 1470. | I: |
| 1471. | S: TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos |
| keladi | |
| 1472. | +: Tramsport |
| 1473. | -:Kanal, Fizik |
| 1474. | -:Tarmoq |
| 1475. | -:Ilova, taqdimot, seans. |
| 1476. | I: |
| 1477. | S: TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos |
| keladi | |
| 1478. | +: Ilova, taqdimot, seans |
| 1479. | -:Kanal, Fizik |
| 1480. | -:Tarmoq |
| 1481. | -:Tramsport |

### 1482. I:

1483. S: Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.

1484. +: Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.

1485. -:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.

1486. -:Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi

1487. -:Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi

### 1488. I:

1489. S: Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.

1490. +: Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.

1491. -:Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.

1492. -:Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi

1493. -:Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi.

### 1494. I:

1495. S: Repetir nima?

1496. +: Odatda signalni tiklash yoki qaytarish uchun foydalaniladi

1497. -:Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi

1498. -: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi

1499. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi

### 1500. I:

1501. S: Hub nima?

1502. +: Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi

1503. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi, Odatda signalni tiklash yoki qaytarish uchun foydalaniladi

1504. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.

1505. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi

### 1506. I:

1507. S: Router nima?

1508. +: Qabul qilingan ma’lumotlarni tarmoq satxiga tegishli manzillarga ko‘ra (IP manzil) uzatadi.

1509. -:Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi

1510. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.

1511. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi

### 1512. I:

1513. S: Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi

1514. +: Razvedka hujumlari 1515. -:Kirish hujumlari

1516. -:DOS hujumi

1517. -:Zararli hujumlar

### 1518. I:

1519. S: Razvedka hujumiga berilgan ta’rifni aniqlang

1520. +: Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;

1521. -:hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi hujumchi -:mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;

|  |  |
| --- | --- |
| 1522. | -:zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi; |
| 1523. | I: |
| 1524. | S: OSI modelining birinchi satxi qanday nomlanadi |
| 1525. | +: Fizik satx |
| 1526. | -:Seanslar satxi |
| 1527. | -:Transport satxi |
| 1528. | -:Taqdimlash satxi |
| 1529. | I: |
| 1530. | S: OSI modelining ikkinchi satxi qanday nomlanadi |
| 1531. | +: Kanal satxi |
| 1532. | -:Amaliy satxi |
| 1533. | -:Fizik satx |
| 1534. | -:Seanslar satxi |
| 1535. | I: |
| 1536. | S: OSI modelining uchinchi satxi qanday nomlanadi |
| 1537. | +: Tarmoq satxi |
| 1538. | -:Amaliy satx |
| 1539. | -:Kanal satxi |
| 1540. | -:Taqdimlash satxi |
| 1541. | I: |
| 1542. | S: OSI modelining oltinchi satxi qanday nomlanadi |
| 1543. | +: Taqdimlash satxi |
| 1544. | -:Amaliy satx |
| 1545. | -:Seanslar satxi |
| 1546. | -:Kanal satxi |
| 1547. | I: |
| 1548. | S: OSI modelining ettinchi satxi qanday nomlanadi |
| 1549. | +: Amaliy satx |
| 1550. | -:Seanslar satxi |
| 1551. | -:Transport satxi |

|  |  |
| --- | --- |
| 1552. | -:Taqdimlash satxi |
| 1553. | I: |
| 1554. | S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining |
| qaysi satxi bajaradi | |
| 1555. | +: Fizik satx |
| 1556. | -:Kanal satxi |
| 1557. | -:Tarmoq satxi |
| 1558. | -:Transport satxi |
| 1559. | I: |
| 1560. | S: Keltirilgan protokollarning qaysilari transport satxi protokollariga |
| mansub | |
| 1561. | +: TCP,UDP |
| 1562. | -:NFS, FTP |
| 1563. | -:IP, IPX |
| 1564. | -:Ethernet, FDDI |
| 1565. | I: |
| 1566. | S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi |
| 1567. | +: Elektr signallarini uzatish va qabul qilish |
| 1568. | -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni |
| boshqarish | |
| 1569. | -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash |
| 1570. | -:Klient dasturlari bilan o’zaro muloqotda bo’lish |
| 1571. | I: |
| 1572. | S: OSI modelining amaliy satxi qanday funksiyalarni bajaradi |
| 1573. | +: Klient dasturlari bilan o’zaro muloqotda bo’lish |
| 1574. | -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni |
| boshqarish | |
| 1575. | -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash |
| 1576. | -:Elektr signallariniuzatish va qabul qilish |
| 1577. | I: |
| 1578. | S: Yevklid algoritmi qanday natijani beradi? |
| 1579. | +: Sonning eng katta umumiy bo’luvchisini toppish |
| 1580. | -:Sonning turli bo’luvchilarini toppish |
| 1581. | -:Sonning eng kichik umumiy karralisini toppish |
| 1582. | -:Sonning eng katta umumiy bo’linuvchisini topish |
| 1583. | I: |
| 1584. | S: Qanday sonlar tub sonlar deb yuritiladi? |
| 1585. | +: Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi. |
| 1586. | -:O’zidan boshqa bo’luvchilari mavjud bo’lgan sonlar tub sonlar deyiladi. |
| 1587. | -:Agar sonning 1 dan boshqa bo’luvchilari bo’lsa. |
| 1588. | -:Faqatgina 1 ga o’ziga bo’linmaydigan sonlar tub sonlar deyiladi. |
| 1589. | I: |
| 1590. | S: OSI modelining birinchi satxi qanday nomlanadi |
| 1591. | +: Fizik satx |
| 1592. | -:Seanslar satxi |
| 1593. | -:Transport satxi |
| 1594. | -:Taqdimlash satxi |
| 1595. | I: |

|  |  |
| --- | --- |
| 1596. | S: OSI modelining ikkinchi satxi qanday nomlanadi |
| 1597. | +: Kanal satxi |
| 1598. | -:Amaliy satxi |
| 1599. | -:Fizik satx |
| 1600. | -:Seanslar satxi |
| 1601. | I: |
| 1602. | S: OSI modelining uchinchi satxi qanday nomlanadi |
| 1603. | +: Tarmoq satxi |
| 1604. | -:Amaliy satx |
| 1605. | -:Kanal satxi |
| 1606. | -:Taqdimlash satxi |
| 1607. | I: |
| 1608. | S: OSI modelining oltinchi satxi qanday nomlanadi |
| 1609. | +: Taqdimlash satxi |
| 1610. | -:Amaliy satx |
| 1611. | -:Seanslar satxi |
| 1612. | -:Kanal satxi |
| 1613. | I: |
| 1614. | S: OSI modelining ettinchi satxi qanday nomlanadi |
| 1615. | +: Amaliy satx |
| 1616. | -:Seanslar satxi |
| 1617. | -:Transport satxi |
| 1618. | -:Taqdimlash satxi |
| 1619. | I: |
| 1620. | S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining |
| qaysi satxi bajaradi | |
| 1621. | +: Fizik satx |
| 1622. | -:Kanal satxi |
| 1623. | -:Tarmoq satxi |
| 1624. | -:Transport satxi |
| 1625. | I: |
| 1626. | S: Keltirilgan protokollarning qaysilari transport satxi protokollariga |
| mansub | |
| 1627. | +: TCP,UDP |
| 1628. | -:NFS, FTP |
| 1629. | -:IP, IPX |
| 1630. | -:Ethernet, FDDI |
| 1631. | I: |
| 1632. | S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi |
| 1633. | +: Elektr signallarini uzatish va qabul qilish |
| 1634. | -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni |
| boshqarish | |
| 1635. | -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash |
| 1636. | -:Klient dasturlari bilan o’zaro muloqotda bo’lish |
| 1637. | I: |
| 1638. | S: OSI modeliningamaliy satxi qanday funktsiyalarni bajaradi |
| 1639. | +: Klient dasturlari bilan o’zaro muloqotda bo’lish |

1640. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni

|  |  |
| --- | --- |
| boshqarish | |
| 1641. | -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash |
| 1642. | -:Elektr signallariniuzatish va qabul qilish |
| 1643. | I: |
| 1644. | S: Yevklid algoritmi qanday natijani beradi? |
| 1645. | +: Sonning eng katta umumiy bo’luvchisini toppish |
| 1646. | -:Sonning turli bo’luvchilarini toppish |
| 1647. | -:Sonning eng kichik umumiy karralisini toppish |
| 1648. | -:Sonning eng katta umumiy bo’linuvchisini topish |
| 1649. | I: |
| 1650. | S: Qanday sonlar tub sonlar deb yuritiladi? |
| 1651. | +: Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi. |
| 1652. | -:O’zidan boshqa bo’luvchilari mavjud bo’lgan sonlar tub sonlar deyiladi. |
| 1653. | -:Agar sonning 1 dan boshqa bo’luvchilari bo’lsa. |
| 1654. | -:Faqatgina 1 ga o’ziga bo’linmaydigan sonlar tub sonlar deyiladi. |
| 1655. | I: |
| 1656. | S: Antivirus dasturlarini ko’rsating? |
| 1657. | +: Drweb, Nod32, Kaspersky |
| 1658. | -:arj, rar, pkzip, pkunzip |
| 1659. | -:winrar, winzip, winarj |
| 1660. | -:pak, lha |
| 1661. | I: |
| 1662. | S: Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan |
| foydalaniladi | |
| 1663. | +: wep, wpa, wpa2 |
| 1664. | -:web, wpa, wpa2 |
| 1665. | -:wpa, wpa2 |
| 1666. | -:wpa, wpa2, wap |
| 1667. | I: |
| 1668. | S: Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak? |
| 1669. | +: ishonchli, qimmatli va to’liq |
| 1670. | -:uzluksiz va uzlukli |
| 1671. | -:ishonchli, qimmatli va uzlukli |
| 1672. | -:ishonchli, qimmatli va uzluksiz |
| 1673. | I: |
| 1674. | S: Axborotning eng kichik o’lchov birligi nima? |
| 1675. | +: bit |
| 1676. | -:kilobayt |
| 1677. | -:bayt |
| 1678. | -:bitta simvol |
| 1679. | I: |
| 1680. | S: Virtual xususiy tarmoq – bu? |
| 1681. | +: VPN |
| 1682. | -:APN |
| 1683. | -:ATM |
| 1684. | -:Ad-hoc |
| 1685. | I: |

1686. S: Xavfli viruslar bu - …

1687. +: kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar 1688. -:tizimda mavjudligi turli taassurot (ovoz, video) bilan bog’liq viruslar,

bo’sh xotirani kamaytirsada, dastur va ma`lumotlarga ziyon yetkazmaydi 1689. -:o’z-o’zidan tarqalish mexanizmi amalga oshiriluvchi viruslar

1690. -:dastur va ma`lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o’chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar

### 1691. I:

1692. S: Mantiqiy bomba – bu …

1693. +: Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari

1694. -:Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari 1695. -:Viruslar kodiga boshqarishni uzatish

1696. -:Qidirishning passiv mexanizmlarini amalga oshiruvchi, yahni dasturiy fayllarga tuzoq qo’yuvchi viruslar

### 1697. I:

1698. S: Rezident virus...

1699. +: tezkor xotirada saqlanadi

1700. -:to’liqligicha bajarilayotgan faylda joylashadi 1701. -:ixtiyoriy sektorlarda joylashgan bo’ladi 1702. -:alohida joyda joylashadi

### 1703. I:

1704. S: DIR viruslari nimani zararlaydi? 1705. +: FAT tarkibini zararlaydi

1706. -:com, exe kabi turli fayllarni zararlaydi 1707. -:yuklovchi dasturlarni zararlaydi

1708. -:Operatsion tizimdagi sonfig.sys faylni zararlaydi 1709. I:

1710. S: kompyuter tarmoqlari bo’yicha tarqalib, komlg’yuterlarning

tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi 1711. +: «Chuvalchang» va replikatorli virus

1712. -:Kvazivirus va troyan virus 1713. -:Troyan dasturi

1714. -:Mantiqiy bomba

### 1715. I:

1716. S: Fire Wall ning vazifasi...

1717. +: tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi

1718. -:kompyuterlar tizimi xavfsizligini ta`minlaydi

1719. -:Ikkita kompyuter o’rtasida aloqa o’rnatish jarayonida Internet tarmog’i orasida xavfsizlikni ta`minlaydi

1720. -:uy tarmog’i orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi

|  |  |
| --- | --- |
| 1721. | I: |
| 1722. | S: Kompyuter virusi nima? |
| 1723. | +: maxsus yozilgan va zararli dastur |
| 1724. | -:.exe fayl |

|  |  |
| --- | --- |
| 1725. | -:boshqariluvchi dastur |
| 1726. | -:Kengaytmaga ega bo’lgan fayl |
| 1727. | I: |
| 1728. | S: Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating |
| 1729. | +: disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali |
| 1730. | -: faqat maxsus tashuvchi qurilma orqali |
| 1731. | -: faqat kompyuter tarmoqlari orqali |
| 1732. | -:zararlanish yo’llari juda ko’p |
| 1733. | I: |
| 1734. | S: Troyan dasturlari bu... |
| 1735. | +: virus dasturlar |
| 1736. | -:antivirus dasturlar |
| 1737. | -:o’yin dasturlari |
| 1738. | -:yangilovchi dasturlar |
| 1739. | I: |
| 1740. | S: Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? |
| 1741. | +: 5 |
| 1742. | -:4 |
| 1743. | -:2 |
| 1744. | -:3 |
| 1745. | I: |
| 1746. | S: Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud |
| 1747. | +: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar |
| 1748. | -:detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar |
| 1749. | -:vaktsinalar, privivkalar, revizorlar, tekshiruvchilar |
| 1750. | -:privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar |
| 1751. | I: |
| 1752. | S: Stenografiya mahnosi... |
| 1753. | +: sirli yozuv |
| 1754. | -:sirli xat |
| 1755. | -:maxfiy axborot |
| 1756. | -:maxfiy belgi |
| 1757. | I: |
| 1758. | S: …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida |
| stenografiyaning bazasi hisoblanadi | |
| 1759. | +: K.Shennon |
| 1760. | -:Sezar |
| 1761. | -:U.Xill |
| 1762. | -:Fon Neyman |
| 1763. | I: |
| 1764. | S: Kriptologiya yo’nalishlari nechta? |
| 1765. | +: 2 |
| 1766. | -:3 |
| 1767. | -:4 |
| 1768. | -:5 |
| 1769. | I: |
| 1770. | S: Kriptografiyaning asosiy maqsadi... |
| 1771. | +: maxfiylik, yaxlitlilikni ta`minlash |

|  |  |
| --- | --- |
| 1772. | -:ishonchlilik, butunlilikni ta`minlash |
| 1773. | -:autentifikatsiya, identifikatsiya |
| 1774. | -:ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya |
| 1775. | I: |
| 1776. | S: DES algoritmi akslantirishlari raundlari soni qancha? |
| 1777. | +: 16; |
| 1778. | -:14; |
| 1779. | -:12; |
| 1780. | -:32; |
| 1781. | I: |
| 1782. | S: DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining |

o‘lchami qancha?

1783. +: CHap qism blok 32 bit, o‘ng qism blok 32 bit; 1784. -:CHap qism blok 32 bit, o‘ng qism blok 48 bit; 1785. -:CHap qism blok 64 bit, o‘ng qism blok 64 bit; 1786. -:CHap qism blok 16 bit, o‘ng qism blok 16 bit; 1787. I:

1788. S: 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta? 1789. +: 18 ta;

1790. -:19 ta

1791. -:11 ta

1792. -:9 ta

### 1793. I:

1794. S: 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta? 1795. +: 3 ta

1796. -:7 ta

1797. -:8 ta;

1798. -:9 ta

### 1799. I:

1800. S: Qaysi formula qoldiqli bo’lish qonunini ifodalaydi 1801. +: a = *bq + r,* 0 ≤ r ≤ b ,

1802. -:𝑎 = 𝑝𝑎1𝑝𝑎2𝑝𝑎3 … 𝑝𝑎𝑘

1 2 3 𝑘

1803. -:M=r1^k2;

### 1804. -:M=√𝑘1 + 𝑘2

1805. I:

1806. S: Eyler funksiyasida p=11 va q=13 sonining qiymatini toping. 1807. +: 16

1808. -:59

1809. -:30

1810. -:21

### 1811. I:

1812. S: Eyler funksiyasi yordamida 1811 sonining qiymatini toping. 1813. +: 1810

1814. -:2111

1815. -:16

1816. -:524

### 1817. I:

1818. S: 97 tub sonmi?

|  |  |  |
| --- | --- | --- |
| 1819. | +: Tub |  |
| 1820. | -:murakkab |
| 1821. | -:Natural |
| 1822. | -:To’g’ri javob yo’q |
| 1823. | I: |
| 1824. | S: Quyidagi modulli ifodani qiymatini toping |
| 1825. | (148 + 14432) mod 256. |
| 1826. | +: 244 |
| 1827. | -:200 |
| 1828. | -:156 |
| 1829. | -:154 |
| 1830. | I: |
| 1831. | S: Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. | 88 i 220 |
| 1832. | +: 44 |  |
| 1833. | -:21 |  |
| 1834. | -:42 |  |
| 1835. | -:20 |  |
| 1836. | I: |  |
| 1837. | S: Quyidagi ifodani qiymatini toping. -16mod11 |  |
| 1838. | +: 6 |  |
| 1839. | -:5 |  |
| 1840. | -:7 |  |
| 1841. | -:11 |  |
| 1842. | I: |  |
| 1843. | S: 2 soniga 10 modul bo’yicha teskari sonni toping. |  |
| 1844. | +: Ø |  |
| 1845. | -:3 |  |
| 1846. | -:10 |  |
| 1847. | -:25 |  |
| 1848. | I: |  |
| 1849. | S: 2 soniga 10 modul bo’yicha teskari sonni toping. |  |
| 1850. | +: Ø |  |
| 1851. | -:3 |  |
| 1852. | -:10 |  |
| 1853. | -:25 |  |
| 1854. | I: |  |
| 1855. | S: DES da dastlabki kalit uzunligi necha bitga teng? |  |
| 1856. | +:56 bit |  |
| 1857. | -:128 bit |  |
| 1858. | -:64 bit |  |
| 1859. | -:32 bit |  |
| 1860. | I: |  |
| 1861. | S: DES da bloklar har birining uzunligi necha bitga teng? |  |
| 1862. | +:32 bit |  |
| 1863. | -:56 bit |  |
| 1864. | -:48 bit |  |
| 1865. | -:64 bit |  |
| 1866. | I: |  |

|  |  |
| --- | --- |
| 1867. | S: DES da raundlar soni nechta? |
| 1868. | +:16 |
| 1869. | -:32 |
| 1870. | -:8 |
| 1871. | -:48 |
| 1872. | I: |
| 1873. | S: Shifrlash kaliti noma’lum bo’lganda shifrlangan ma’lumotni deshifrlash |
| qiyinlik darajasini nima belgilaydi | |
| 1874. | +:kriptobardoshlik |
| 1875. | -:Shifr matn uzunligi |
| 1876. | -:Shifrlash algoritmi |
| 1877. | -:Texnika va texnologiyalar |
| 1878. | I: |
| 1879. | S: Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga |
| bo’linadi | |
| 1880. | +:blokli va oqimli |
| 1881. | -:DES va oqimli |
| 1882. | -:Feystel va Verman |
| 1883. | -:SP− tarmoq va IP |
| 1884. | I: |
| 1885. | S: DES shifrlash algoritmida shifrlanadigan malumotlar bloki necha bit? |
| 1886. | +:64 |
| 1887. | -:32 |
| 1888. | -:48 |
| 1889. | -:56 |
| 1890. | I: |
| 1891. | S: XOR amali qanday amal? |
| 1892. | +:2 modul bo`yicha qo`shish |
| 1893. | -:264 modul bo`yicha qo`shish |
| 1894. | -:232 modul bo`yicha qo`shish |
| 1895. | -:248 modul bo`yicha qo`shish |
| 1896. | I: |
| 1897. | S: 4+31 mod 32 ? |
| 1898. | +:3 |
| 1899. | -:4 |
| 1900. | -:31 |
| 1901. | -:32 |
| 1902. | I: |
| 1903. | S: 21+20mod32? |
| 1904. | +:9 |
| 1905. | -:12 |
| 1906. | -:16 |
| 1907. | -:41 |
| 1908. | I: |
| 1909. | S: 12+22 mod 32 ? |
| 1910. | +:2 |
| 1911. | -:12 |
| 1912. | -:22 |

|  |  |
| --- | --- |
| 1913. | -:32 |
| 1914. | I: |
| 1915. | S: AES algoritmi bloki uzunligi … bitdan kam bo’lmasligi kerak. |
| 1916. | +:128 |
| 1917. | -:512 |
| 1918. | -:256 |
| 1919. | -:192 |
| 1920. | I: |
| 1921. | S: Xesh-:funktsiyani natijasi … |
| 1922. | +:fiksirlangan uzunlikdagi xabar |
| 1923. | -:Kiruvchi xabar uzunligidagi xabar |
| 1924. | -:Kiruvchi xabar uzunligidan uzun xabar |
| 1925. | -:fiksirlanmagan uzunlikdagi xabar |
| 1926. | I: |
| 1927. | S: 2+5 mod32 ? |
| 1928. | +:7 |
| 1929. | -:32 |
| 1930. | -:2 |
| 1931. | -:5 |
| 1932. | I: |
| 1933. | S: 97 tub sonmi? |
| 1934. | +:Tub |
| 1935. | -:murakkab |
| 1936. | -:Natural |
| 1937. | -:To’g’ri javob yo’q |
| 1938. | I: |
| 1939. | S: Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga |
| o’tkazing. | |
| 1940. | +:23 |
| 1941. | -:20 |
| 1942. | -:21 |
| 1943. | -:19 |
| 1944. | I: |
| 1945. | S: Quyidagi ifodani qiymatini toping. -17mod11 |
| 1946. | +:5 |
| 1947. | -:6 |
| 1948. | -:7 |
| 1949. | -:11 |
| 1950. | I: |
| 1951. | S: Diskni shifrlash nima uchun amalga oshiriladi? |
| 1952. | +: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini |

ta’minlash uchun amalga oshiriladi

1953. -:Xabarni yashirish uchun amalga oshiriladi

1954. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi

1955. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi

### 1956. I:

|  |  |
| --- | --- |
| 1957. | S: Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi? |
| 1958. | +: 4 |
| 1959. | -:8 |
| 1960. | -:7 |
| 1961. | -:5 |
| 1962. | I: |
| 1963. | S: OSI modelida nechta tarmoq satxi bor |
| 1964. | +: 7 |
| 1965. | -:6 |
| 1966. | -:5 |
| 1967. | -:4 |
| 1968. | I: |
| 1969. | S: Diskni shifrlash nima uchun amalga oshiriladi? |
| 1970. | +: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini |

ta’minlash uchun amalga oshiriladi

1971. -:Xabarni yashirish uchun amalga oshiriladi

1972. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi

1973. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi

|  |  |
| --- | --- |
| 1974. | I: |
| 1975. | S: Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi? |
| 1976. | +: 4 |
| 1977. | -:8 |
| 1978. | -:7 |
| 1979. | -:5 |
| 1980. | I: |
| 1981. | S: OSI modelida nechta tarmoq satxi bor |
| 1982. | +: 7 |
| 1983. | -:6 |
| 1984. | -:5 |
| 1985. | -:4 |
| 1986. | I: |
| 1987. | S: “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonun |
| moddadan iborat | |
| 1988. | +:16 |
| 1989. | -:18 |
| 1990. | -:11 |
| 1991. | -:14 |
| 1992. | I: |
| 1993. | S: Kompyuter etikasi instituti notijoriy tashkilot tomonidan texnologiyani |
| axloqiy nuqta nazardan targ‘ib qilish bo‘yicha nechta etika qoidalari keltirilgan | |
| 1994. | +:10 |
| 1995. | -:18 |
| 1996. | -:11 |
| 1997. | -:14 |
| 1998. | I: |
| 1999. | S: Kiberjinoyatchilik bu –. . . |

2000. +: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.

2001. -: Kompyuter o‘yinlari

2002. -: Faqat banklardan pul o‘g‘irlanishi 2003. -: autentifikatsiya jarayonini buzish 2004. I:

2005. S: Fishing nima?

2006. +: Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

|  |  |
| --- | --- |
| 2007. | -: Ma’lumotlar bazalarini xatoligi |
| 2008. | -: Mualliflik huquqini buzilishi |
| 2009. | -: Lug‘at orqali xujum qilish. |
| 2010. | I: |
| 2011. | S: Bag nima? |
| 2012. | +: Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan |
| muammo | |
| 2013. | -: Mualliflik huquqini buzilishi |
| 2014. | -: Dasturlardagi ortiqcha reklamalar |
| 2015. | -: Autentifikatsiya jarayonini buzish |
| 2016. | I: |
| 2017. | S: Nuqson nima? |
| 2018. | +: Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi |
| nuqsondir | |
| 2019. | -: Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo |
| 2020. | -: Dasturlardagi ortiqcha reklamalar |
| 2021. | -: Autentifikatsiya jarayonini buzish |
| 2022. | I: |
| 2023. | S: Quyidagilardan qaysi birida xavfsiz dasturlash tillari keltirilgan. |
| 2024. | +: C#, Scala, Java |
| 2025. | -: C, C#, java |
| 2026. | -: C++, Scala, Java |
| 2027. | -: Misra-C, Java, c++ |
| 2028. | I: |
| 2029. | S: Quyidagilardan qaysi biri dasturiy maxsulotlarga qo‘yiladigan xavfsizlik |
| talablari hisoblanidi. | |
| 2030. | +: Vazifaviy, novazifaviy, qolgan talablar |
| 2031. | -: Qolgan talablar, anaviy taablar, etika talablari |
| 2032. | -: Vazifaviy, novazifaviy, etika talablari. |
| 2033. | -: Vazifaviy, etika talablari, foydalanuvchanlik talablari. |
| 2034. | I: |
| 2035. | S: Dasturiy ta’minotda kirish va chiqishga aloqador bo‘lgan talablar |
| qanday talablar sirasiga kiradi? | |
| 2036. | +:Vazifaviy |
| 2037. | -: Novazifaviy |
| 2038. | -: Etika talablari |
| 2039. | -: Qolgan talablar |
| 2040. | I: |

|  |  |
| --- | --- |
| 2041. | S: Dasturda tizim amalga oshirishi kerak bo‘lgan vazifalar bu.. |
| 2042. | +:Vazifaviy |
| 2043. | -: Novazifaviy |
| 2044. | -: Etika talablari |
| 2045. | -: Qolgan talablar |
| 2046. | I: |
| 2047. | S: Risklarni boshqarishda risklarni aniqlash jarayoni bu-.. |
| 2048. | +: Tashkilot xavfsizligiga ta’sir qiluvchi tashqi va ichki risklarning |

manbasi, sababi, oqibati va haklarni aniqlash.

2049. -: Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta’siri va ehtimolini o‘lchashni ta’minlaydi.

2050. -: Risklarni davolash bu – aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni.

2051. -: Risk monitoringi yangi risklarni paydo bo‘lish imkoniyatini aniqlash. 2052. I:

2053. S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.

2054. +:"Sovuq saxiralash"

2055. -:"Issiq zaxiralash"

2056. -:"Iliq saxiralash"

2057. -:"To'liq zaxiralash"

### 2058. I:

2059. S: Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishi bilan bog'liq bo'lsa bu nima deb yuritiladi?

2060. +:Jinoyat sifatida baholanadi 2061. -:Rag’bat hisoblanadi

2062. -:Buzgunchilik hisoblanadi 2063. -:Guruhlar kurashi hisoblanadi 2064. I:

2065. S: Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun qanday kalit ishlatiladi?

2066. +:Ikkita kalit

2067. -:Bitta kalit

2068. -:Elektron raqamli imzo 2069. -:Foydalanuvchi identifikatori

### 2070. I:

2071. S:Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

2072. +:Axborot xavfsizligi buzulgan taqdirda ko’rilishi mumkin bo’lgan zarar miqdori bilan

2073. -:Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhumligi bilan

2074. -:Axborotni noqonuniy foydalanishlardan o’zgartirishlardan va yo’q qilishlardan himoyalanganligi bilan

2075. -:Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bilan}

### 2076. I:

2077. S:Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

|  |  |
| --- | --- |
| 2078. | +:Strukturalarni ruxsatsiz modifikatsiyalash |
| 2079. | -:Tabiy ofat va avariya |
| 2080. | -:Texnik vositalarning buzilishi va ishlamasligi |
| 2081. | -:Foydalanuvchilar va xizmat ko‘rsatuvchi hodimlarning hatoliklari} |
| 2082. | I: |
| 2083. | S:Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy |
| tahdidlar deb hisoblanadi? | |
| 2084. | +:Texnik vositalarning buzilishi va ishlamasligi |
| 2085. | -:Axborotdan ruhsatsiz foydalanish |
| 2086. | -:Zararkunanda dasturlar |
| 2087. | -:An’anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili} |
| 2088. | I: |
| 2089. | S:Axborot xavfsizligini ta'minlovchi choralarni ko’rsating? |
| 2090. | +:1-huquqiy, 2-tashkiliy-ma'muriy, 3-injener-texnik |
| 2091. | -:1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy |
| 2092. | -:1-dasturiy, 2-tashkiliy-ma'muriy, 3-huquqiy |
| 2093. | -:1-aparat, 2-texnikaviy, 3-huquqiy} |
| 2094. | I: |
| 2095. | S:Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o’z ichiga |
| oladi  2096. +:Xalqaro va milliy huquqiy me’yorlarni | |
| 2097. | -:Tashkiliy va xalqaro me’yorlarni |
| 2098. | -:Ananaviy va korporativ me’yorlarni |
| 2099. | -:Davlat va nodavlat tashkilotlarime’yorlarni} |
| 2100. | I: |
| 2101. | S:Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki |
| mazmunini saqlash xususiyati nima deb ataladi? | |
| 2102. | +: Ma’lumotlar butunligi |
| 2103. | -:Axborotning konfedensialligi |
| 2104. | -:Foydalanuvchanligi |
| 2105. | -:Ixchamligi} |
| 2106. | I: |
| 2107. | S:Axborotning buzilishi yoki yo‘qotilishi xavfiga olib keluvchi |
| himoyalanuvchi ob’ektga qarshi qilingan xarakatlar qanday nomlanadi? | |
| 2108. | +:Tahdid |
| 2109. | -:Zaiflik |
| 2110. | -:Hujum |
| 2111. | -:Butunlik} |
| 2112. | I: |
| 2113. | S:Biometrik autentifikatsiyalashning avfzalliklari-bu: |
| 2114. | +:Biometrik alomatlarning noyobligi |
| 2115. | -:Bir marta ishlatilishi |
| 2116. | -:Biometrik alomatlarni o’zgartirish imkoniyati |
| 2117. | -:Autentifikatsiyalash jarayonining soddaligi |
| 2118. | I: |
| 2119. | S: Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar |

axborotdan foydalana olishliklari-bu:

|  |  |
| --- | --- |
| 2120. | +:Foydalanuvchanligi |
| 2121. | -:Ma’lumotlar butunligi |
| 2122. | -:Axborotning konfedensialligi |
| 2123. | -:Ixchamligi |
| 2124. | I: |
| 2125. | S:Global simsiz tarmoqning ta`sir doirasi qanday? |
| 2126. | +:Butun dunyo bo’yicha |
| 2127. | -:Binolar va korpuslar |
| 2128. | -:O’rtacha kattalikdagishahar |
| 2129. | -:Foydalanuvchi yaqinidagi tarmoq |
| 2130. | I: |
| 2131. | S: Foydalanuvchini identifikatsiyalashda qanday ma’lumotdan |
| foydalaniladi? | |
| 2132. | +:Identifikatori |
| 2133. | -:Telefon raqami |
| 2134. | -:Parol |
| 2135. | -:Avtorizatsiyasi |
| 2136. | I: |
| 2137. | S: Foydalanuvchining tarmoqdagi harakatlarini va resurslardan |
| foydalanishga urinishini qayd etish-bu: | |
| 2138. | +:Ma`murlash |
| 2139. | -:Autentifikatsiya |
| 2140. | -:Identifikatsiya |
| 2141. | -:Sertifikatsiyalash |
| 2142. | I: |
| 2143. | S: Kompyuter tizimini ruxsatsiz foydalanishdan himoyalashni, muhim |

kompyuter tizimlarni rezervlash, o‘g‘irlash va diversiyadan himoyalanishni ta’minlash rezerv elektr manbai, xavfsizlikning maxsus dasturiy va apparat vositalarini ishlab chiqish va amalga oshirish qaysi choralarga kiradi?

|  |  |
| --- | --- |
| 2144. | +:Injener-texnik |
| 2145. | -:Molyaviy |
| 2146. | -:Tashkiliy-ma’muriy |
| 2147. | -:Huquqiy |
| 2148. | I: |
| 2149. | S: Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy |
| ekanligini tekshirish muolajasi-bu: | |
| 2150. | +:Autentifikatsiya |
| 2151. | -:Identifikatsiya |
| 2152. | -:Ma`murlash (accaunting) |
| 2153. | -:Avtorizatsiya |
| 2154. | I: |
| 2155. | S: O‘zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari |
| va komandalaridan foydalanadi–bu: | |
| 2156. | +:Tarmoq viruslari |
| 2157. | -:Pochta viruslari |
| 2158. | -:Fayl viruslari |
| 2159. | -:Protokol viruslari |
| 2160. | I: |

|  |  |
| --- | --- |
| 2161. | S: Qanday viruslar xavfli hisoblanadi? |
| 2162. | +:kompyuter ishlashida jiddiy nuqsonlarga olib keluvchi |
| 2163. | -:Jiddiy nuqsonlarga olib kelmaydigan ammo foydalanuvchini |
| chalg'itadigan. | |
| 2164. | -:Katta viruslar va odatda zararli dasturlar |
| 2165. | -:Passiv viruslar |
| 2166. | I: |
| 2167. | S: Rezident bo’lmagan viruslar qachon xotirani zararlaydi? |
| 2168. | +:Faqat faollashgan vaqtida |
| 2169. | -:Faqat o’chirilganda |
| 2170. | -:Kompyuter yoqilganda |
| 2171. | -:Tarmoq orqali ma’lumot almashishda |
| 2172. | I: |
| 2173. | S: Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan iborat? |
| 2174. | +:Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud |
| 2175. | -:Tarmoq chetki nuqtalari orasidagi xududning kengligi asosida |

qurilmalarholati

2176. -:Himoya vositalarining chegaralanganligi

2177. -:Himoyani amalga oshirish imkoniyati yo‘qligi va ma'lum protokollarning ishlatilishi

### 2178. I:

2179. S: Simmetrik shifrlashning noqulayligi – bu:

2180. +:Maxfiy kalitlar bilan ayirboshlash zaruriyatidir 2181. -:Kalitlar maxfiyligi

2182. -:Kalitlar uzunligi

2183. -:SHifrlashga ko‘p vaqt sarflanishi va ko'p yuklanishi 2184. I:

2185. S: Simsiz tarmoqlarni kategoriyalarini to’g’ri ko’rsating?

2186. +:Simsiz shaxsiy tarmoq (PAN), simsiz lokal tarmoq (LAN), simsiz regional tarmoq (MAN) va Simsiz global tarmoq (WAN)

2187. -:Simsiz internet tarmoq (IAN )va Simsiz telefon tarmoq (WLAN), Simsiz shaxsiy tarmoq (PAN) va Simsiz global tarmoq (WIMAX)

|  |  |
| --- | --- |
| 2188. | -:Simsiz internet tarmoq (IAN) va uy simsiz tarmog’i |
| 2189. | -:Simsiz chegaralanmagan tarmoq (LAN), simsiz kirish nuqtalari |
| 2190. | I: |
| 2191. | S: Sub`ektga ma`lum vakolat va resurslarni berish muolajasi-bu: |
| 2192. | +:Avtorizatsiya |
| 2193. | -:Haqiqiylikni tasdiqlash |
| 2194. | -:Autentifikatsiya |
| 2195. | -:Identifikasiya |
| 2196. | I: |
| 2197. | S: Tarmoq operatsion tizimining to'g'ri konfiguratsiyasini madadlash |
| masalasini odatda kim hal etadi? | |
| 2198. | +:Tizim ma'muri |
| 2199. | -:Tizim foydalanuvchisi |
| 2200. | -:Korxona raxbari |
| 2201. | -:Operator |

|  |  |
| --- | --- |
| 2202. | I: |
| 2203. | S: Tarmoqlararo ekran texnologiyasi-bu: |
| 2204. | +:Ichki va tashqi tarmoq o’rtasida filtr va himoya vazifasini bajaradi |
| 2205. | -:Ichki va tashqi tarmoq o’rtasida axborotni o’zgartirish vazifasini bajaradi |
| 2206. | -:Qonuniy foydalanuvchilarni himoyalash |
| 2207. | -:Ishonchsiz tarmoqdan kirishni boshqarish} |
| 2208. | I: |
| 2209. | S: Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini |
| ko’rsating? | |
| 2210. | +:DDoS (Distributed Denial of Service) hujum |
| 2211. | -:Tarmoq hujumlari |
| 2212. | -:Dastur hujumlari asosidagi (Denial of Service) hujum |
| 2213. | -:Virus hujumlari} |
| 2214. | I: |
| 2215. | S: Uyishtirilmagan tahdid, ya’ni tizim yoki dasturdagi qurilmaning jismoniy |
| xatoligi – bu… | |
| 2216. | +:Tasodifiy tahdid |
| 2217. | -:Uyishtirilgan tahdid |
| 2218. | -:Faol tahdid |
| 2219. | -:Passiv tahdid |
| 2220. | I: |
| 2221. | S: Axborot xavfsizligi qanday asosiy xarakteristikalarga ega? |
| 2222. | +:Butunlik, konfidentsiallik, foydalana olishlik |
| 2223. | -:Butunlik, himoya, ishonchlilikni urganib chiqishlilik |
| 2224. | -:Konfidentsiallik, foydalana olishlik |
| 2225. | -:Himoyalanganlik, ishonchlilik, butunlik |
| 2226. | } |
| 2227. | I: |
| 2228. | S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay |
| turganda zahiralash amalga oshirilsa …. deb ataladi. | |
| 2229. | +:"Sovuq saxiralash" |
| 2230. | -:"Issiq zaxiralash" |
| 2231. | -:"Iliq saxiralash" |
| 2232. | -:"To'liq zaxiralash" |
| 2233. | I: |
| 2234. | S: Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham |
| zahiralash amalga oshirilishi …. deb ataladi? | |
| 2235. | +:"Issiq zaxiralash" |
| 2236. | -:"Sovuq saxiralash" |
| 2237. | -:"Iliq saxiralash" |
| 2238. | -:"To'liq zaxiralash" |
| 2239. | I: |
| 2240. | S: Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang |
| 2241. | +:HandyBakcup |
| 2242. | -:Recuva, R.saver |
| 2243. | -:Cryptool |
| 2244. | -:Eset32 |
| 2245. | I: |

|  |  |
| --- | --- |
| 2246. | S: O'chirilgan, formatlangan ma'lumotlarni tikovchi dasturni belgilang. |
| 2247. | +:Recuva, R.saver |
| 2248. | -:HandyBakcup |
| 2249. | -:Cryptool |
| 2250. | -:Eset32 |
| 2251. | I: |
| 2252. | S: Virtuallashtirishga qaratilgan dasturiy vositalarni belgilang. |
| 2253. | +:VMware, VirtualBox |
| 2254. | -:HandyBakcup |
| 2255. | -:Eset32 |
| 2256. | -:Cryptool |
| 2257. | I: |
| 2258. | S: Cloud Computing texnologiyasi nechta katta turga ajratiladi? |
| 2259. | +:3 turga |
| 2260. | -:2 turga |
| 2261. | -:4 turga |
| 2262. | -:5 turga |
| 2263. | I: |
| 2264. | S: O'rnatilgan tizimlar-bu… |
| 2265. | +:Bu ko'pincha real vaqt hisoblash cheklovlariga ega bo'lgan kattaroq |

mexanik yoki elektr tizimidagi maxsus funksiyaga ega, boshqaruvchidir 2266. -:Korxona ichki tarmog’iga ulangan korporativ tarmog’idan bo'ladigan

hujumlardan himoyalash

2267. -:Korxona ichki tarmog’ini Internet global tarmog’idan ajratib qo’yish 2268. -:Bu ko'pincha global tizimda hisoblash cheklovlariga ega bo'lgan mexanik

yoki elektr tizimidagi maxsus funksiyaga ega qurilmadir 2269. I:

2270. S: Axborotdan oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan?

|  |  |
| --- | --- |
| 2271. | +:AQSH sog'liqni saqlash va insonlarga xizmat ko'rsatish vazirligi |
| 2272. | -:AQSH Mudofaa vazirligi |
| 2273. | -:O'zbekiston Axborot texnologiyalari va kommunikatsiyalarni |
| rivojlantirish vazirligi | |
| 2274. | -:Rossiya kiberjinoyatlarga qarshu kurashish davlat qo'mitasi |
| 2275. | I: |
| 2276. | S: Axborotdan oqilona foydalanish kodeksi nechanchi yil ishlab chiqilgan? |
| 2277. | +:1973 yil |
| 2278. | -:1980 yil |
| 2279. | -:1991 yil |
| 2280. | -:2002 yil |
| 2281. | I: |
| 2282. | S: Kompyuter bilan bog'liq falsafiy soha bo'lib, foydalanuvchilarning xatti- |
| harakatlari, komyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko'rsatishini o'rgatadigan soha nima deb ataladi? | |
| 2283. | +:Kiberetika |
| 2284. | -:Kiberhuquq |
| 2285. | -:Kiberqoida |
| 2286. | -:Kiberxavfsizlik |

### 2287. I:

2288. S: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…

2289. +:Kiberjinoyat

2290. -:Kibersport

2291. -:Kiberterror

2292. -:Hakerlar uyushmasi

### 2293. I:

2294. S: Tarmoqlararo ekran paket filtrlari qaysi sathda ishlaydi? 2295. +:Tarmoq sathida

2296. -:Ilova sathida

2297. -:Kanal sathida

2298. -:Fizik sathida

### 2299. I:

2300. S: Tarmoqlararo ekran ekspert paketi filtrlari qaysi sathda ishlaydi? 2301. +:Transport sathida

2302. -:Ilova sathida

2303. -:Kanal sathida

2304. -:Fizik sathida

### 2305. I:

2306. S: Spam bilan kurashishning dasturiy uslubida nimalar ko’zda tutiladi? 2307. +:Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida

filtrlanib cheklanadi

2308. -:Elektron pochta qutisiga kelib tushadigan spamlar me’yoriy xujjatlar asosida cheklanadi va bloklanadi

2309. -:Elektron pochta qutisiga kelib tushadigan spamlar ommaviy ravishda cheklanadi

2310. -:Elektron pochta qutisiga kelib spamlar mintaqaviy hududlarda cheklanadi 2311. I:

2312. S: Ma’lumotlarni yo’qolish sabab bo’luvchi tabiiy tahdidlarni ko’rsating 2313. +:Zilzila, yong‘in, suv toshqini va hak

2314. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

2315. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi

2316. -:Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani

### 2317. I:

2318. S: Ma’lumotlarni tasodifiy sabablar tufayli yo’qolish sababini belgilang 2319. +:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani

to‘satdan zararlanishi

2320. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi

2321. -:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

2322. -:Zilzila, yong‘in, suv toshqini va hak 2323. I:

2324. S: Ma’lumotlarni inson xatosi tufayli yo’qolish sababini belgilang.

2325. +:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

2326. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi

2327. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

2328. -:Zilzila, yong‘in, suv toshqini va hak 2329. I:

2330. S: Ma’lumotlarni g’arazli hatti harakatlar yo’qolish sababini ko’rsating. 2331. +:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki

o‘g‘irlanishi

2332. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

2333. -:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

2334. -:Zilzila, yong‘in, suv toshqini va hak 2335. I:

2336. S: Kompyuterda hodisalar haqidagi ma’lumot qayerda saqlanadi? 2337. +:Hodisalar jurnaliga

2338. -:Operativ xotiraga

2339. -:Kesh xotiraga

2340. -:Vaqtinchalik faylga

### 2341. I:

2342. S: Internet orqali masofada joylashgan kompyuterga yoki tarmoq resurslariga DoS hujumlari uyushtirilishi natijasida..

2343. +:Foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan mahrum qilinadilar

2344. -:Foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzg’unchilarga etkaziladi

2345. -:Axborot tizimidagi ma’lumotlar bazalari o’g’irlanib ko’lga kiritilgach, ular yo’q qilinadilar

2346. -:Foydalanuvchilar axborotlariga ruxsatsiz o’zgartirishlar kiritilib, ularning yaxlitligi buziladi

### 2347. I:

2348. S: Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo’naltirilgan buzg’unchi bu - ... .

|  |  |
| --- | --- |
| 2349. | +:Krakker |
| 2350. | -:Hakker |
| 2351. | -:Virus bot |
| 2352. | -:Ishonchsiz dasturchi |
| 2353. | I: |
| 2354. | S: Antivirus dasturiy vositalari viruslarni tahlil qilishiga ko'ra necha turga |
| bo'linadi? | |
| 2355. | +:2 turga: fayl Signaturaga va evristikaga asoslangan |
| 2356. | -:2 turga: faol va passiv |
| 2357. | -:2 turga: pulli va pulsiz |
| 2358. | -:2 turga: litsenziyali va ochiq |
| 2359. | I: |

|  |  |
| --- | --- |
| 2360. | S: "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat? |
| 2361. | +:Foydalanish davrida maxfiylik kamayib boradi |
| 2362. | -:Parolni esda saqlash kerak bo'ladi |
| 2363. | -:Parolni almashtirish jarayoni murakkabligi |
| 2364. | -:Parol uzunligi soni cheklangan |
| 2365. | I: |
| 2366. | S: Yaxlitlikni buzilishi bu - … |
| 2367. | +:Soxtalashtirish va o’zgartirish |
| 2368. | -:Ishonchsizlik va soxtalashtirish |
| 2369. | -:Soxtalashtirish |
| 2370. | -:Butunmaslik va yaxlitlanmaganlik |
| 2371. | I: |
| 2372. | S: Tarmoqda joylashgan fayllar va boshqa resurslardan foydalanishni |
| taqdim etuvchi tarmoqdagi kompyuter nima? | |
| 2373. | +:Server |
| 2374. | -:Bulutli tizim |
| 2375. | -:Superkompyuter |
| 2376. | -:Tarmoq |
| 2377. | I: |
| 2378. | S: Tahdid nima? |
| 2379. | +:Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan |
| hodisa. | |
| 2380. | -:Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa |
| 2381. | -:Bu riskni o‘zgartiradigan harakatlar bo‘lib |
| 2382. | -:Bu noaniqlikning maqsadlarga ta’siri |
| 2383. | I: |
| 2384. | S: Risk nima? |
| 2385. | +:Potensial kuchlanish yoki zarar |
| 2386. | -:Potensial foyda yoki zarar |
| 2387. | -:Tasodifiy taxdid |
| 2388. | -:Katta yo‘qotish |
| 2389. | I: |
| 2390. | S: Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi? |
| 2391. | +:Optik tolali |
| 2392. | -:O’rama juft |
| 2393. | -:Koaksial |
| 2394. | -:Telefon kabeli |
| 2395. | I: |
| 2396. | S: Nima uchun autentifikatsiyalashda parol ko’p qo’llaniladi? |
| 2397. | +:Sarf xarajati kam, almashtirish oson |
| 2398. | -:Parolni eslab qolish oson |
| 2399. | -:Parolni o’g’rishlash qiyin |
| 2400. | -:Serverda parollarni saqlash oson |
| 2401. | I: |
| 2402. | S: Elektron xujjatlarni yo’q qilish usullari qaysilar? |
| 2403. | +:Shredirlash, magnitsizlantirish, yanchish |
| 2404. | -:Yoqish, ko’mish, yanchish |
| 2405. | -:Shredirlash, yoqish, ko’mish |

|  |  |
| --- | --- |
| 2406. | -:Kimyoviy usul, yoqish. |
| 2407. | I: |
| 2408. | S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? |
| 2409. | +:Imzo qo‘yish va imzoni tekshirishdan |
| 2410. | -:Faqat imzo qo‘yishdan |
| 2411. | -:Faqat imzoni tekshirishdan |
| 2412. | -:Kalitlarni taqsimlashdan |
| 2413. | I: |
| 2414. | S: Elektron pochtaga kirishda foydalanuvchi qanday autetntifikasiyalashdan |
| o’tadi? | |
| 2415. | +:Parol asosida |
| 2416. | -:Smart karta asosida |
| 2417. | -:Biometrik asosida |
| 2418. | -:Ikki tomonlama |
| 2419. | I: |
| 2420. | S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Jazolar |

bosqichiga to‘g‘ri ta’rif berilgan.

2421. -: tashkilot o‘z siyosatini ishlab chiqishdan oldin o‘z aktivlari uchun risklarni baholashi shart

2422. -: tashkilot o‘z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o‘rnatilish shart

2423. -: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo‘shimcha kiritish jarayonida boshqaruvchi bo‘lishi shart

2424. +: ma’lum tashkilotlarda tashkilotlarda qat’iy siyosatlar mavjud. Agar xodimlar ushbu siyosatlarga amal qilmasa, ularga qarshi bir qancha choralar qo‘llaniladi.

### 2425. I:

2426. S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Xodimlarni o‘rgatish bosqichiga to‘g‘ri ta’rif berilgan.

2427. -: tashkilot o‘z siyosatini ishlab chiqishdan oldin o‘z aktivlari uchun risklarni baholashi shart

2428. -: tashkilot o‘z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o‘rnatilish shart

2429. -: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo‘shimcha kiritish jarayonida boshqaruvchi bo‘lishi shart

2430. +: xodimlarga tashkilot xavfsizlik siyosati davomli ravishda o‘rgatilishi shart

### 2431. I:

2432. S: Galstuk babochka usuli nima? 2433. +: Risklarni baholash usuli 2434. -: Risklarni qabul qilish usuli 2435. -: shifrlash algoritmi

2436. -: Risklarni hosil qilish usuli. 2437. I:

2438. S: Lotin alifbosida DADA so‘zini 3 kalit bilan shifrlagandan so‘ng qaysi so‘z hosil bo‘ladi. A=0, B=1….Z=25.

### 2439. +:GDGD

2440. -: NANA

|  |  |
| --- | --- |
| 2441. | -: GPGP |
| 2442. | -: FDFD |
| 2443. | I: |
| 2444. | S: Lotin alifbosida NON so‘zini 3 kalit bilan shifrlagandan so‘ng qaysi so‘z |
| hosil bo‘ladi. A=0, B=1….Z=25. | |
| 2445. | -:GDGD |
| 2446. | -: NANA |
| 2447. | +: QRQ |
| 2448. | -: FDFD |
| 2449. | I: |
| 2450. | S: Fizik to‘siqlarni o‘rnatish , Xavfsizlik qo‘riqchilarini ishga olish, Fizik |
| qulflar qo‘yishni amalga oshirish qanday nazorat turiga kiradi? | |
| 2451. | +:Fizik nazorat |
| 2452. | -: Texnik nazorat |
| 2453. | -: Ma’muriy nazorat |
| 2454. | -: Tashkiliy nazorat |
| 2455. | I: |
| 2456. | S: Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish |

tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?

2457. -: Fizik nazorat 2458. +:Texnik nazorat 2459. -: Ma’muriy nazorat 2460. -: Tashkiliy nazorat 2461. I:

2462. S: Qoida va muolajalarni yaratish, Joylashuv arxitekturasini loyihalash, Xavfsizlik belgilari va ogohlantirish signallari, Ishchi joy xavfsizligini ta’minlash, Shaxs xavfsizligini ta’minlash amalga oshirish qanday nazorat turiga kiradi?

|  |  |
| --- | --- |
| 2463. | -: Fizik nazorat |
| 2464. | -: Texnik nazorat |
| 2465. | +: Ma’muriy nazorat |
| 2466. | -: Tashkiliy nazorat |
| 2467. | I: |
| 2468. | S: Ikkilik sanoq tizimida qanday raqamlardan foydalanamiz? |
| 2469. | +: Faqat 0 va 1 |
| 2470. | -: Faqat 1 |
| 2471. | -: Faqat 0 |
| 2472. | -: Barcha raqamlardan |
| 2473. | I: |
| 2474. | S: AES shifrlash algoritmi necha rounddan iborat |
| 2475. | +: 10, 12, 14 |
| 2476. | -: 10,14,16 |
| 2477. | -: 12,14,16 |
| 2478. | -: 16 |
| 2479. | I: |
| 2480. | S: Hodisalar daraxti usuli nima? |
| 2481. | +: Risklarni baholash usuli |

|  |  |
| --- | --- |
| 2482. | -: Risklarni qabul qilish usuli |
| 2483. | -: shifrlash algoritmi |
| 2484. | -: Risklarni hosil qilish usuli |
| 2485. | I: |
| 2486. | S: Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib |
| shifrlagan? | |
| 2487. | +:3 taga |
| 2488. | -:4 taga |
| 2489. | -:2 taga |
| 2490. | -:5 taga |
| 2491. | I: |
| 2492. | S: WiMAX qanday simsiz tarmoq turiga kiradi. |
| 2493. | +: Regional |
| 2494. | -: Lokal |
| 2495. | -: Global |
| 2496. | -: Shaxsiy |
| 2497. | I: |
| 2498. | S: Wi-Fi necha Gs chastotali to'lqinda ishlaydi? |
| 2499. | +: 2.4-5 Gs |
| 2500. | -: 2.4-2.485 Gs |
| 2501. | -: 1.5-11 Gs |
| 2502. | -: 2.3-13.6 Gs |
| 2503. | I: |
| 2504. | S: Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi? |
| 2505. | +: Onx458&hdsh) |
| 2506. | +: 12456578 |
| 2507. | +: salomDunyo |
| 2508. | +: Mashina777 |
| 2509. | I: |
| 2510. | S: Parollash siyosatiga ko'ra parol tanlash shartlari qanday? |
| 2511. | +: Kamida 8 belgi: katta va kichik xavflar, sonlar , kamida bitta maxsus |

simvol qo'llanishi kerak. -: Kamida 8 belgi: katta va kichik xavflar, sonlar qo'llanishi kerak.

2512. -: Kamida 6 belgi: katta xarflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak.

2513. -: Kamida 6 belgi: katta va kichik xarflar, kamida bitta maxsus simvol qo'llanishi kerak.

Dqw

2. Windows otda necha turdagi hodisa ro‘yxatga olinadi?  
  
1. Axborot xavfsizligining asosiy maqsadlaridan biri-bu…   
Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish   
2. Windows OTda necha turdagi hodisa ro‘yxatga olinadi?   
a) 5 ta   
3. Konfidentsiallikga to‘g‘ri ta’rif keltiring.   
a) axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;   
4. Kriptografiya faninining asosiy maqsadi nima?   
a) maxfiylik, yaxlitlilikni ta’minlash   
5. Kriptografiyada kalitning vazifasi nima?   
b) Matnni shifrlash va shifrini ochish uchun kerakli axborot   
6. Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq?   
a) simmetrik kriptotizimlar   
7. Autentifikatsiya nima?   
a) Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi   
8. Identifikatsiya bu- …   
a) Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni   
9. Kriptobardoshlilik deb nimaga aytilladi?   
a) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi   
10. Kriptografiyada matn –bu..   
a) alifbo elementlarining tartiblangan to‘plami

11. Kriptotizimga qo‘yiladigan umumiy talablardan biri nima?

a) shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak   
12. Berilgan ta’riflardan qaysi biri assimetrikrik tizimlarga xos?   
a) Assimetrikrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

13. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…

a) login   
14. Uning egasi haqiqiyligini aniqlash jarayonida matnhiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?   
a) parol   
15. Ro‘yxatdan o‘tish-bu…   
a) foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni   
16. Axborot qanday sifatlarga ega bo‘lishi kerak?   
a) ishonchli, qimmatli va to‘liq

17. Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish nima deb ataladi?

b) steganografiya   
18. Kriptografiya fan sifatida shakllanishida nechta davrlarga bo‘linadi?   
a) 4 ga

19. Shifrmatntni ochiq matntga akslantirish jarayoni nima deb ataladi?

a) Deshifrlash   
20. Risk-tushunchasi nima?   
a) Belgilangan sharoitda tahdidning manbalarga bo‘lishi mumkin bo‘lgan zarar yetkazilishini kutish   
21. Tahdid-tushunchasi nima?   
a) Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa   
22. Kodlash terminiga berilgan ta’rifni belgilang.   
a) Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir   
23. Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug‘ullanadi?   
b) Kriptoanaliz   
24. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?   
a) {d, n} – yopiq, {e, n} – ochiq;   
25. Zamonaviy kriptografiya qanday bo‘limlardan iborat?   
a) Simmetrik kriptotizimlar; Ochiq kalitli kriptotizimlar; Elektron raqamli imzo; Kalitlarni boshqarish   
26. Shifr nima?   
a) Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm   
27. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?   
b) Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi   
28. Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?   
c) Xesh funksiyalar   
29. Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...   
a) Avtorizatsiya   
30. Autentifikatsiya faktorlari nechta?   
b) 3 ta   
31. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?   
a) Biometrik autentifikatsiya   
32. Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini belgilaydigan atamani toping.   
b) Kriptobardoshlik   
33. Qog‘oz ma’lumotlarni yo‘q qilish odatda necha xil usuldan foydalaniladi?   
a) 4 xil   
34. Kiberjinoyat qanday turlarga bo‘linadi?   
a) Ichki va tashqi   
35. “Kiberxavfsizlik to‘g‘risida” Qonun qachon tasdiqlangan?   
a) 15.04.2022 y   
36. Kiberjinoyatchilik bu –. . .   
a) Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.   
37. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?   
d) Texnik vositalarning buzilishi va ishlamasligi   
38. Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?   
c) Ma’lumotlar butunligi   
39. Biometrik autentifikatsiyalashning avfzalliklari-bu:   
b) Biometrik parametrlarning noyobligi   
40. Simmetrik shifrlashning noqulayligi – bu:   
a) Maxfiy kalitlar bilan ayirboshlash zaruriyatidir   
41. Token, smartkartalarda xavfsizlik tomonidan kamchiligi nimada?   
a) Foydalanish davrida maxfiylik kamayib boradi   
b) Qurilmalarni ishlab chiqarish murakkab jarayon   
**c) Qurilmani yo‘qotilishi katta xavf olib kelishi mumkin**   
d) Qurilmani qalbakilashtirish oson

42. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating

a) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi   
**b) Zilzila, yong‘in, suv toshqini va hak.**   
c) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi   
d) Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani

43. Ma’lumotlarni tasodifiy sabablar tufayli yo‘qolish sababini belgilang

**a) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi**   
b) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi   
c) Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.   
d) Zilzila, yong‘in, suv toshqini va hak.

44. Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.

a) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi.   
**b) Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.**   
c) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi   
d) Zilzila, yong‘in, suv toshqini va hak.

45. "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?

a) Parolni esda saqlash kerak bo‘ladi.   
b) Parolni almashtirish jarayoni murakkabligi   
c) Parol uzunligi soni cheklangan   
**d) Foydalanish davrida maxfiylik kamayib boradi**

46. Nima uchun autentifikatsiyalashda parol ko‘p qo‘llaniladi?

**a) Sarf xarajati kam, almashtirish oson**   
b) Parolni foydalanubchi ishlab chiqadi   
c) Parolni o‘g‘rishlash qiyin   
d) Serverda parollar saqlanmaydi

47. Elektron xujjatlarni yo‘q qilish usullari qaysilar?

a) Yoqish, ko‘mish, yanchish   
**b) Shredirlash, magnitsizlantirish, yanchish**   
c) Shredirlash, yoqish, ko‘mish   
d) Kimyoviy usul, yoqish.

48. Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?

a) 4 taga   
b) 2 taga   
c) 5 taga   
**d) 3 taga**

49. Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi?

**a) Knx1@8&h**   
b) qwertyu   
c) salomDunyo   
d) Mashina505

50. Parollash siyosatiga ko‘ra parol tanlash shartlari qanday?

a) Kamida 7 belgi; katta va kichik xavflar, sonlar qo‘llanishi kerak.   
**b) Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo‘llanishi kerak.**   
c) Kamida 6 belgi; katta xarflar, sonlar , kamida bitta maxsus simvol qo‘llanishi kerak.   
d) Kamida 6 belgi; katta va kichik xarflar, kamida bitta maxsus simvol qo‘llanishi kerak.

51. MD5, SHA1, SHA256, O‘z DSt 1106:2009- qanday algoritmlar deb ataladi?

a) Kodlash   
**b) Xeshlash**   
c) Shifrlash   
d) Stenografiya

52. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

a) O‘rta asr davrida   
b) 15 asr davrida   
**c) 1-2 jahon urushu davri**   
d) 21 asr davrida

53. "Fishing" tushunchasi-bu…:

a) Kompyuter va kompyuter tarmoqlarida odamlarning etikasi   
b) Kompyuter, dasturlar va tarmoqlar xavfsizligi   
**c) Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi**   
d) Kompyuter tizimlariga ruxsatsiz ta’sir ko‘rsatish

54. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?

a) Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyot.   
b) Hisoblash tizimi xizmatlaridan foydalanish huqu kiberxavfsizlik qiga ega shaxs (shaxslar guruxi, tashkilot).   
**c) Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar**   
d) Ma’lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo‘ljallangan dasturiy va apparat vositalar

55. Axborot xavfsizligi timsollarini ko‘rsating.

a) Haker, Krakker   
**b) Alisa, Bob, Eva**   
c) Buzg‘unchi, hujumchi   
d) subyekt, user

56. Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.

**a) Qonunlar**   
b) Qarorlar   
c) Standartlar   
d) Farmonlar

57. Qaysi siyosat tizim resurslarini foydalanishda hech qanday cheklovlar qo‘ymaydi?

a) Ruxsat berishga asoslangan siyosat   
b) Paranoid siyosat   
c) Extiyotkorlik siyosati   
**d) Nomuntazam siyosat**

58. “Hаmmа nаrsа tа’qiqlаnаdi.” Bu qаysi xаvfsizlik siyosаtigа xos?

a) Ruxsаt berishgа аsoslаngаn siyosаt (Permissive Policy)   
**b) Pаrаnoid siyosаti (Pаrаnoid Policy)**   
c) Ehtiyotkorlik siyosаti (Prudent Policy)   
d) Nomuntаzаm siyosаt (Promiscuous Policy

59. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…

a) Kibersport deb ataladi   
b) Kiberterror deb ataladi   
**c) Kiberjinoyat deb ataladi**   
d) Hakerlar uyushmasi deyiladi

60. Qaysi siyosat turli hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi?

**a) Maqbul foydalanish siyosati**   
b) Paranoid siyosat   
c) Ruxsat berishga asoslangan siyosat   
d) Nomuntazam siyosat

61. Qaysi siyosatda Adminstrator xavfsiz va zarur xizmatlarga indvidual ravishda ruxsat beradi?

a) Paranoid siyosat   
b) Ruxsat berishga asoslangan siyosat   
c) Nomuntazam siyosat   
**d) Extiyotkorlik siyosati**

62. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?

a) Nomuntazam siyosat   
b) Paranoid siyosat   
**c) Ruxsat berishga asoslangan siyosat**   
d) Extiyotkorlik siyosati

63. Qaysi siyosatga ko‘ra hamma narsa taqiqlanadi?

a) Ruxsat berishga asoslangan siyosat   
b) Nomuntazam siyosat   
c) Extiyotkorlik siyosati   
**d) Paranoid siyosat**

64. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima deyiladi?

**a) Xavfsizlik siyosat**   
b) Standart   
c) Qaror   
d) Buyruq

65. Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to‘liq tasavvurga ega shaxs kim deb ataladi?

a) Xavfsizlik mutaxasisi   
b) Rahbar   
c) Foydalanuvchi   
**d) Xavfsizlik ma'muri (admin)**

66. Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o‘z ichiga oladi?

**a) Xalqaro va milliy huquqiy me’yorlarni**   
b) Tashkiliy va xalqaro me’yorlarni   
c) Ananaviy va korporativ me’yorlarni   
d) Davlat va nodavlat tashkilotlari me’yorlarni

67. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….

a) Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi   
b) Hamma narsa ta’qiqlanadi   
c) Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi   
**d) Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi**

68. ... - faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot.

**a) Parol**   
b) Login   
c) Maxfiy kalit   
d) Shifrlangan axborot

69. “Dasturiy ta’minotlar xavfsizligi” bilim sohasi - bu ...

**a) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.**   
**b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.**   
c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.   
d) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

70. “Jamoat xavfsizligi” bilim sohasi - bu …

**a) u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi.**   
b) tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini   
c) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi   
d) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

71. “Ma’lumotlar xavfsizligi” bilim sohasi - bu …

**a) ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.**   
b) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi   
c) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.   
d) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

72. “Tizim xavfsizligi” bilim sohasi - bu …

**a) tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi.**   
b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.   
c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.   
d) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

73. “Xodim xavfsizligi” tushunchasi- bu…

**a) Qandaydir jiddiy axborotdan foydalanish imkoniyatiga ega barcha xodimlarning kerakli avtorizatsiyaga va barcha kerakli ruxsatnomalarga egalik kafolatini ta’minlovchi usul.**   
b) Axborot tarmog‘ini ruxsatsiz foydalanishdan, me’yoriy harakatiga tasodifan aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.   
c) Destruktiv harakatlarga va yolg‘on axborotni zo‘rlab qabul qilinishiga olib keluvchi ishlanadigan va saqlanuvchi axborotdan ruxsatsiz foydalanishga urinishlarga kompyuter tizimining qarshi tura olish hususiyati.   
d) Korxona o‘z faoliyatini buzilishsiz va to‘xtalishsiz yurgiza oladigan vaqt bo‘yicha barqaror bashoratlanuvchi atrof-muhit holati.

74. “Yaxlitlik” atamasiga berilgan ta’rifni belgilang.

**a) Bu yozilgan va xabar qilingan ma’luotlarning haqiqiyligini, to‘g‘riligini, butunligini saqlash qobiliyati**   
b) Funksionala imkoniyatni o‘z vaqtida foydalanish   
c) Tizimning ruxsat berilgan foydalanish uchun ma’lumot tarqatishni cheklash   
d) Korxona o‘z faoliyatini buzilishsiz va to‘xtalishsiz yurgiza oladigan vaqt bo‘yicha barqaror bashoratlanuvchi atrof-muhit holati

75. ……–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

**a) Kiberxavfsizlik**   
b) Axborot xavfsizligi   
c) Kiberjtnoyatchilik   
d) Risklar

76. Assimetrikrik kriptotizimlarda axborotni shifrlashda va deshifrlash uchun qanday kalit ishlatiladi?

**a) Ikkita kalit: ochiq va yopiq**   
b) Bitta kalit   
c) Elektron raqamli imzo   
d) Foydalanuvchi identifikatori

77. Autentifikatsiya jarayoni qanday jarayon?

**a) obyekt yoki subyektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy axborotni tekshirish orqali asilligini aniqlash**   
b) axborot tizimlari obyekt va subyektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo‘yicha solishtirib uni aniqlash jarayoni   
c) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni   
d) foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni

78. Avtorizatsiya nima?

a) Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilarga tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni   
b) Subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim qilish jarayoni   
c) Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni   
d) Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilar

79. Axborot o‘lchovini kamayish tartibini to‘g‘ri tanlang

a) Terabayt,gigabayt,megabayt   
b) Bit,bayt,kilobayt,megabayt   
c) Gigabayt,megabayt,bayt   
d) Gigabayt,megabayat,terobayt

80. Axborot o‘lchovini o‘sish tartibini to‘g‘ri tanlang

a) Kilobayt,megabayt,gigabayt   
b) Bit,bayt,megabayt,kilobayt   
c) Gigabayt,megabayt,pikobayt   
d) Gigabayt,terabayt,pikobayt

81. Axborot xavfsizligi qanday asosiy xarakteristikalarga ega?

a) Butunlik, konfidentsiallik, foydalanuvchanlik   
b) Butunlik, himoya, ishonchlilikni o‘rganib chiqishlilik   
c) Konfidentsiallik, foydalana olishlik   
d) Himoyalanganlik, ishonchlilik, butunlik

82. Axborot xavfsizligining huquqiy ta'minotiga nimalar kiradi?

a) Qonunlar, aktlar, me'yoriy-huquqiy hujjatlar, qoidalar, yo‘riqnomalar, qo‘llanmalar majmui   
b) Qoidalar yo‘riqnomalar, tizim arxetikturasi, xodimlar malakasi, yangi qoidalar, yangi yo‘riqnomalar, qo‘llanmalar majmui   
c) Qoidalar, yo‘riqnomalar, tizim strukturasi, dasturiy ta’minot   
d) Himoya tizimini loyihalash, nazorat usullari

83. "Barcha xizmatlar blokirovka qilingandan so‘ng bog‘lanadi". -Bu qaysi xavfsizlik siyosatiga hos?

a) Ehtiyotkorlik siyosati (Prudent Policy)   
b) Nomuntazam siyosat (Promiscuous Policy)   
c) Paranoid siyosati (Paranoid Policy)   
d) Ruxsat berishga asoslangan siyosat (Permissive Policy)

84. Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo‘linadi?

a) Blokli va oqimli   
b) DES va oqimli   
c) Feystel va Verman   
d) SP− tarmoq va IP

85. BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?

a) AES, Serpent, Twofish   
b) Pleyfer, Sezar   
c) DES, sezar, Futurama   
d) AES, Serpent, Twofish, Triple DES, GOST 28147-89

86. Blokli shifrlash tushunchasi nima?

a) shifrlanadigan matn blokiga qo‘llaniladigan asosiy akslantirish   
b) murakkab bo‘lmagan kriptografik akslantirish   
c) axborot simvollarini boshqa alfavit simvollari bilan almashtirish   
d) ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi

87. Elektron pochtaga kirishda foydalanuvchi qanday autetntifikasiyalashdan o‘tadi?

a) Parol asosida   
b) Smart karta asosida   
c) Biometrik asosida   
d) Ikki tomonlama

88. Elektron raqamli imzo - bu …

a) xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimcha   
b) matnni shifrlash va shifrini ochish uchun kerakli axborot   
c) axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam   
d) kalit axborotni shifrlovchi kalitlar

89. Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?

a) Imzo qo‘yish va imzoni tekshirishdan   
b) Faqat imzo qo‘yishdan   
c) Faqat imzoni tekshirishdan   
d) Kalitlarni taqsimlashdan

90. Elektron raqamli imzo kalitlari ro‘yxatga olish qaysi tashkilot tomonidan bajariladi

a) Sertifikatlari roʻyxatga olish markazlari   
b) Tegishli Vazirliklar   
c) Axborot xavfsizligi markazlari   
d) Davlat Hokimiyati

91. Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima?

a) Autentifikatsiya   
b) Identifikatsiya   
c) Avtorizatsiya   
d) Ma’murlash

92. Kriptografiyada kalit – bu …

a) Matnni shifrlash va shifrini ochish uchun kerakli axborot   
b) Bir qancha kalitlar yig‘indisi   
c) Axborotli kalitlar to‘plami   
d) Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

93. Kiberetika tushunchasi-bu…

a) Kompyuter va kompyuter tarmoqlarida odamlarning etikasi   
b) Kompyuter, dasturlar va tarmoqlar xavfsizligi   
c) Kompyuter tizimlariga ruxsatsiz ta’sir ko‘rsatish   
d) Tashkilot va odamlarning mahsus va shahsiy ma’lumotlarini olishka qaratilgan internet-atakasi

94. Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi?

a) tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi   
b) tashkilot xodimlari himoyasini ta’minlaydi   
c) tashkilot axborotlari va binolarining himoyasini ta’minlaydi   
d) tashkilot omborini va axborotlari himoyasini ta’minlaydi

95. Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda qo‘llaniladi?

a) ochiq kalitlar   
b) yopiq kalitlar   
c) seans kalitlari   
d) Barcha tutdagi kalitlar

96. Kriptografiyada "alifbo" deganda nima tushuniladi?

a) axborotni ifodalashda ishlatiluvchi bilgilarning chekli to‘plami tushuniladi   
b) matnni shifrlash va shifrini ochish uchun kerakli axborot   
c) xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimcha   
d) alfavit elementlaridan tartiblangan nabor

97. O‘zbekistonda masofadan elektron raqamli imzo olish uchun qaysi internet manzilga murojaat qilinadi?

a) e-imzo.uz   
b) elektron-imzo.uz   
c) imzo.uz   
d) eri.uz

98. Oqimli shifrlashning mohiyati nimada?

a) Oqimli shifrlash birinchi navbatda axborotni bloklarga bo‘lishning imkoni bo‘lmagan hollarda zarur,   
b) Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo‘natish uchun oqimli shifrlash zarur,   
c) Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo‘yicha shifrlaydi   
d) Oqimli shifrlash birinchi navbatda axborotni bloklarga bo‘lishning imkoni bo‘lgan hollarda zarur,

99. RSA algoritmi qanday jarayonlardan tashkil topgan?

a) Kalitni generatsiyalash; Shifrlash; Deshifrlash.   
b) Shifrlash; Imzoni tekshirish; Deshifrlash   
c) Kalitni generatsiyalash; imzolash; Deshifrlash.   
d) Imzoni tekshirish ; Shifrlash; Deshifrlash.

100. Shaxsning, o‘zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, axborot-kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu?

a) login   
b) parol   
c) identifikatsiya   
d) maxfiy maydon

101. Shifrlash qanday jarayon?

a) akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi   
b) kalit asosida shifrmatn ochiq matnga akslantiriladi   
c) shifrlashga teskari jarayon   
d) almashtirish jarayoni bo‘lib: ochiq matn deb nomlanadigan matn o‘girilgan holatga almashtiriladi

102. Kichik xajmdagi xotira va hisoblash imkoniyatiga ega bo‘lgan, o‘zida parol yoki kalitni saqlovchi qurilma nima deb ataladi?

a) Token, Smartkarta   
b) Chip   
c) Fleshka   
d) Disk

103. Cisco tashkiloti “kiberxavfsizlik” atamasiga qanday ta’rif bergan?

a) Kiberxavfsizlik - tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti   
b) Hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan   
c) Bu yozilgan va xabar qilingan ma’luotlarning haqiqiyligini, to‘g‘riligini, butunligini saqlash qobiliyati   
d) Ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.

104. Foydalanuvchanlik-bu…

a) avtorizatsiyalangan mantiqiy obyekt so‘rovi bo‘yicha axborotning tayyorlik va foydalanuvchanlik holatida bo‘lishi xususiyati   
b) axborotning buzilmagan ko‘rinishida (axborotning qandaydir qayd etilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati   
c) axborot yoki uni eltuvchisining shunday holatiki, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi   
d) potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi

105. Kiberxavfsizlik bilim sohasi nechta bilim sohasini o‘z ichiga oladi?

a) 8 ta   
b) 7 ta   
c) 6 ta   
d) 5 ta

106. Ijtimoiy (sotsial) injineriya-bu…

a) turli psixologik usullar va firibgarlik amaliyotining to‘plami, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olish   
b) Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish   
c) axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi   
d) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

107. Kiberxavfsizlik arxitekturasi nechta sathga ajratiladi?

a) 3ta   
b) 2 ta   
c) 4 ta   
d) 5 ta

108. Tashkilot axborot xavfsizligi siyosati-bu…

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.   
b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.   
c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.   
d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

109. Muammoga qaratilgan xavfsizlik siyosatlari …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.   
**b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.**   
c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.   
d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

110. Tizimga qaratilgan xavfsizlik siyosatlari …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.   
b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.   
**c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.**   
d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

111. Internetdan foydalanish siyosati. …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.   
b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.   
c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.   
**d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.**

112. Ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o‘zgartirishlar oilasi-…

**a) Kriptotizim**   
b) Deshifrlash   
c) Rasshifrovkalash   
d) Shifrlash

113. O‘zgartirishlar oilasidan birini tanlashni ta’minlovchi kriptografik algoritmning qandaydir parametrlarining muayyan qiymati-…

a) Kriptotizim   
**b) Kalit**   
c) Rasshifrovkalash   
d) Shifrlash

114. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuning maqsadi nimadan iborat?

a) Har kimning axborotni erkin va moneliksiz izlash, olish, tadqiq etish, uzatish hamda tarqatishga doir konstitutsiyaviy huquqini amalga oshirish jarayonida yuzaga keladigan munosabatlarni tartibga solish   
b) Axborotlarni maxfiylashtirish va maxfiylikdan chiqarish ushbu Qonunga hamda o‘zbekiston Respublikasi Vazirlar Mahkamasi tasdiqlaydigan ma’lumotlarning maxfiylik darajasini aniqlash va belgilash   
c) Shaxsga doir ma’lumotlar sohasidagi munosabatlarni tartibga solish.   
d) Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.

115. "Axborotlashtirish to‘g‘risida"gi Qonunning maqsadi nimadan iborat?

a) Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.   
b) Shaxsga doir ma’lumotlar sohasidagi munosabatlarni tartibga solish.   
c) Har kimning axborotni erkin va moneliksiz izlash, olish, tadqiq etish, uzatish hamda tarqatishga doir konstitutsiyaviy huquqini amalga oshirish jarayonida yuzaga keladigan munosabatlarni tartibga solish   
d) Axborotlarni maxfiylashtirish va maxfiylikdan chiqarish ushbu Qonunga hamda o‘zbekiston Respublikasi Vazirlar Mahkamasi tasdiqlaydigan ma’lumotlarning maxfiylik darajasini aniqlash va belgilash

116. "Backdoors"-qanday zararli dastur?

a) zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, masalan, administrator parolisiz imtiyozga ega bo‘lish   
b) foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod   
c) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi   
d) marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot

117. .... – o‘zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma’lumoti va xavfsizlik algoritmlarini saqlaydi.

a) Sim karta   
b) Token   
c) Smart karta   
d) Elektron raqamli imzo

118. .... kompyuter tarmoqlari bo‘yicha tarqalib, kompyuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o‘zining nusxasini qoldiradi.

a) “Chuvalchang” va replikatorli virus   
b) Kvazivirus va troyan virus   
c) Troyan dasturi   
d) Mantiqiy bomba

119. “Aloqa xavfsizligi” bilim sohasi - bu …

a) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.   
b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.   
c) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.   
d) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

120. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

a) Foydalanishni boshqarish   
b) Tarmoqni loyihalash   
c) Foydalanish   
d) Identifikatsiya

121. “Inson xavfsizligi” bilim sohasi - bu …

a) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi   
b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi   
c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.   
d) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi

122. “Tashkil etuvchilar xavfsizligi” - bu …

a) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi   
b) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi   
c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi   
d) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi

123. “Tashkilot xavfsizligi” bilim sohasi - bu …

a) tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini   
b) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi   
c) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi   
d) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi

124. …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.

a) UDP   
b) HTTP   
c) TCP   
d) FTP

125. ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.

a) TCP   
b) IP   
c) HTTP   
d) FTP

126. Access control list va Capability list bu nimaning asosiy elementi hisoblanadi?

a) Lampson matritsasining   
b) XASML standartining   
c) Role-based access control RBACning   
d) Attribute based access control (ABAC)ning

127. “Adware” zararli dastur xususiyati nimadan iborat?

a) marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.   
b) foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.   
c) bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi.   
d) o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi

128. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?

a) "Issiq zaxiralash"   
b) "Sovuq saxiralash"   
c) "Iliq saxiralash"   
d) "To‘liq zaxiralash"

129. Qaysi zaxiralash usuli offlayn zaxiralash deb ham atalib, tizim ishlamay turganida yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi?

a) "Sovuq saxiralash"   
b) "Issiq zaxiralash"   
c) "Iliq saxiralash"   
d) "To‘liq zaxiralash"

130. Qaysi zaxiralashda tizim muntazam yangilanishni amalga oshirish uchun tarmoqqa bog‘lanishi kerak bo‘ladi?

a) "Iliq saxiralash"   
b) "Sovuq saxiralash"   
c) "Issiq zaxiralash"   
d) "To‘liq zaxiralash"

131. Agar RSA algotirmida e-ochiq kalitni, d-maxfiy kalitni, n-modul ifodalasa, qaysi formula deshifrlashni ifodalaydi?

a) M = C^d mod n;   
b) C = M^d mod n;   
c) C = M^ed mod n;   
d) M = C^e mod n;

132. Agar RSA algotirmida e-ochiq kalitni, d-maxfiy kalitni, n-modul , qaysi formula shifrlashni ifodalaydi?

a) C = M^e mod n;   
b) C = M^d mod n;   
c) C = M^ed mod n;   
d) M = C^e mod n;

133. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...

a) Tamoqlararo ekranlarning o‘rnatilishi   
b) Tashkiliy ishlarni bajarilishi   
c) Globol tarmoqdan uzib qo‘yish   
d) Aloqa kanallarida optik toladan foydalanish

134. Akslantirish tushunchasi deb nimaga aytiladi?

a) 1-to‘plamli elementlariga 2-to‘plam elementalriga mos bo‘lishiga   
b) 1-to‘plamli elementlariga 2-to‘plam elementalrini qarama-qarshiligiga   
c) har bir elementni o‘ziga ko‘payimasiga   
d) agar birinchi va ikinchi to‘plam bir qiymatga ega bo‘lmasa

135. Antivirus dasturiy vositalari viruslarni tahlil qilishiga ko‘ra necha turga bo‘linadi?

a) 2 turga fayl signaturaga va tahlilga asoslangan   
b) 2 turga faol va passiv   
c) 2 turga pulli va pulsiz   
d) 2 turga litsenziyali va ochiq

136. Antivirus dasturlarini ko‘rsating.

a) Drweb, Nod32, Kaspersky   
b) arj, rar, pkzip, pkunzip   
c) winrar, winzip, winarj   
d) pak, lha

137. Antiviruslar viruslarni asosan qanday usulda aniqlaydi?

a) Signaturaga asoslangan   
b) Anomaliyaga asoslangan   
c) O‘zgarishni aniqlashga asoslangan   
d) Defragmentatsiya qilish

138. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud.

a) detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar   
b) detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar   
c) vaktsinalar, privivkalar, revizorlar, matnhiruvchilar   
d) privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar

139. AQShning axborotni shifrlash standartini keltirilgan javobni ko‘rsating?

a) DES(Data Encryption Standart)   
b) RSA (Rivest, Shamir ва Adleman)   
c) AES (Advanced Encryption Standart)   
d) Aniq standart ishlatilmaydi

140. Assimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?

a) shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun   
b) shifrlash, deshifrlash, kalit generatsiyalash   
c) ERI hosil qilsih, maxfiylikni ta’minlash, kalitlar almashish uchun   
d) shifrlash, deshifrlash, kalitlar boshqarish uchun

141. Assimmetrik kriptotizimlarda axborotni shifrlashda va deshifrlash uchun nechta kalit ishlatiladi?

a) Ikkita kalit   
b) Bitta kalit   
c) Uchta kalit   
d) Foydalanuvchi identifikatori

142. Asosan tarmoq, tizim va tashkilot haqidagi axborotni olish maqasadida amalga oshiriladigan tarmoq hujumini belgilang.

a) Razvedka hujumlari   
b) Kirish hujumlari   
c) DOS hujumi   
d) Zararli hujumlar

143. Atribute based access control ABAC usuli attributlari qaysilar?

a) Foydalanuvchi attributlari   
b) Asosiy va qo‘shimcha atributlar   
c) Tizim attributlari, server atributlari   
d) Ichki va tashqi attributlar

144. Autentifikatsiyaga ta'rif qaysi javobda keltirilgan?

a) Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi   
b) Tizim meyoriy va g‘ayritabiiy hollarda rejalashtirilgandek o‘zini tutishligi holati   
c) Istalgan vaqtda dastur majmuasining mumkinligini kafolati   
d) Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi

145. Avtorizatsiya qanday jarayon?

a) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni   
b) axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo‘yicha solishtirib uni aniqlash jarayoni   
c) obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash.   
d) foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni

146. Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?

a) Korporativ va umumfoydalanuvchi   
b) Regional, korporativ   
c) Lokal, global   
d) Shaharlararo, lokal, global

147. Axborot paketlarini qachon ushlab qolish mumkin?

a) Aloqa kanallari orqali uzatishda   
b) Xotira qurilmalarida saqlanayotganda   
c) Kompyuter ishga tushganda   
d) Ma’lumotlar nusxalanayotganda

148. Axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi nima deb ataladi?

a) Axborot resursi   
b) Axborot xavfsizligi   
c) Ma'lumotlar bazasi   
d) Axborot tizimlari

149. Axborot tizimiga ta’rif bering.

a) Qo‘yilgan maqsadga erishish yo‘lida axborotlarni olish, qayta ishlash, va uzatish uchun usullar, vositalar va xodimlar jamlanmasi   
b) Material olamda axborot almashinuvining yuzaga kelishini ta’minlovchi axborot uzatuvchi, aloqa kanallari, qabul qilgich vositalar jamlanmasi   
c) Qo‘yilgan maqsadga erishish yo‘lida o‘zaro birlashtirilgan va ayni vaqtda yagona deb qaraluvchi elementlar to‘plami   
d) Ishlab chiqarish jarayonida insonlarning umumiy munosabatlarini ifodalovchi vositlar to‘plami

150. Axborot xavfsizligi siyoatining necha xil turi bor?

a) 3   
b) 4   
c) 5   
d) 2

151. Axborot xavfsizligi siyosati –bu …

a) tashkilot o‘z faoliyatida rioya qiladigan axborot xavfsizligi sohasidagi hujjatlangan qoidalar, muolajalar, amaliy usullar yoki amal qilinadigan prinsiplar majmui sanalib, u asosida tashkilotda axborot xavfsizligi ta’minlanadi   
b) mavjud tahdidni amalga oshirilgan ko‘rinishi bo‘lib, bunda kutilgan tahdid amalga oshiriladi   
c) mavjud bo‘lgan zaiflik natijasida bo‘lishi mumkin bo‘lgan hujum turi bo‘lib, ular asosan tizimni kamchiliklarini o‘rganish natijasida kelib chiqadi   
d) tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

152. 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 muhumligi 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

153. Axborot xavfsizligini ta'minlovchi choralarni ko‘rsating?

a) 1-huquqiy, 2-tashkiliy-ma'muriy, 3-dasturiy-texnik   
b) 1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy   
c) 1-amaliy, 2-tashkiliy-ma'muriy, 3-huquqiy   
d) 1-apparat, 2-texnikaviy, 3-huquqiy

154. Axborotdan oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan?

a) AQSH sog‘liqni saqlash va insonlarga xizmat ko‘rsatish vazirligi   
b) AQSH Mudofaa vazirligi   
c) O‘zbekiston Axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi   
d) Rossiya kiberjinoyatlarga qarshu kurashish davlat qo‘mitasi

155. Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?

a) USB fleshka, CD va DVD disklar   
b) Qattiq disklar va CDROM   
c) CD va DVD, kesh xotira   
d) Qattiq disklar va DVDROM

156. Axborotni himoyalash uchun ... usullari qo‘llaniladi.

a) kodlashtirish, kriptografiya, stegonografiya   
b) shifrlash va kriptografiya, maxsus yozilgan kod   
c) Stegonografiya, kriptografiya, orfografiya   
d) Kriptoanaliz, kodlashtirish, zahiralash

157. Axborotning buzilishi yoki yo‘qotilishi xavfiga olib keluvchi himoyalanuvchi obyektga qarshi qilingan xarakatlar qanday nomlanadi?

a) Tahdid   
b) Zaiflik   
c) Hujum   
d) Butunlik

158. Axborotning eng kichik o‘lchov birligi nima?

a) bit   
b) kilobayt   
c) bayt   
d) kilobit

159. Axbоrоt tizimlari xavfsizligining auditi-bu…

a) Axborot tizimlarining himoyalanishining joriy holati, tizim haqida obyektiv ma’lumotlarni olish va baholash   
b) Ma`lumоtlarini tahlillash va chоra ko‘rishni tizim haqida subyektiv ma’lumotlarni olish va baholashni tahlil qiladi   
c) Ma`lumоtlarini tarqatish va boshqarish   
d) Axbоrоtni yig‘ish va korxona tarmog‘ini tahlillash

160. TrueCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?

a) AES, Serpent va Twofish   
b) Serpent, RSA   
c) El-Gamal, Twofish   
d) DES

161. "Bag" atamasini nima ma'noni beradi?

a) Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo   
b) Mualliflik huquqini buzilishi   
c) Dasturlardagi ortiqcha reklamalar   
d) Autentifikatsiya jarayonini buzish

162. "Barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti".- Bular tarmoqning qaysi sathiga kiradi?

a) Fizik sath (physical)   
b) Tarmoq sathi   
c) Amaliy sath   
d) Tadbiqiy sath

163. Bell-LaPadula (BLP) modeli -bu..

a) Bu hukumat va harbiy dasturlarda kirishni boshqarishni kuchaytirish uchun ishlatiladigan avtomatlashgan modeli   
b) Axborlarni nazoratlovchi model   
c) Foydalanuvchilarni ro‘yxatga olish , nazoratlash va tahlil qiluvchi model   
d) Tarmoq boshqarish va tahlil qiluvchi model

164. Bell-LaPadula axborot xavfsizligida axborotni qaysi parametrini ta'minlash uchun xizmat qiladi?

a) Konfidentsiallikni   
b) Yaxlitlikni   
c) Maxfiylikni   
d) O‘zgarmaslikni

165. Biba modeli obyektni qaysi xusuiyatiga e'tibor qaratilgan?

a) Yaxlitligi   
b) Maxfiyligi   
c) Xavfsizligi   
d) Konfidentsialligi

166. BiBa modeli qaysi modelning keygaytirilgan varianti hisoblanadi?

a) Bell-Lapadula modeli   
b) RBAC   
c) MAC   
d) ABAC

167. Biometrik parametrlarda xavfsizlik tomonidan kamchiligi nimadan iborat?

a) ID ni almashtirish murakkabligi   
b) Foydalanish davrida maxfiylik kamayib boradi   
c) Qalbakilashtirish oson   
d) Parol va PIN kod ishlatilmasligi

168. Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang.

a) Shaxsiy simsiz tarmoq   
b) Lokal simsiz tarmoq   
c) Regional simsiz tarmoq   
d) Global simsiz tarmoq

169. Botnet-nima?

a) internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi   
b) zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi   
c) zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish.   
d) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

170. …-bu so‘z ingliz tilidan olingan bo‘lib- yorib tashlash, chopish, buzish degan ma’nolarni anglatadi. Ular xaddan ziyod malakali va bilimli, axborot texnologiyalarini puxta biluvchi insondir.-Yuqoridagi fikr kim to‘g‘risida ta’rif berilgan?

a) Xaker   
b) Dasturchi   
c) Tarmoq josusi   
d) Administrator

171. Bulutli texnologiyalarda PaaS nimani ifodalaydi?

a) Platforma sifatida   
b) Servis sifatida   
c) Ma'lumot sifatida   
d) Prizentatsiya sifatida

172. GSM, GPRS, EDGE, HSPA+, LTE standartida ishlovchi simsiz tarmoq turini aniqlang.

a) Global simsiz tarmoq   
b) Shaxsiy simsiz tarmoq   
c) Lokal simsiz tarmoq   
d) Regional simsiz tarmoq

173. Cloud Computing texnologiyasi nechta katta turga ajratiladi?

a) 3 turga   
b) 2 turga   
c) 4 turga   
d) 5 turga

174. Dastur kodini tashkil qilish yondashuviga ko‘ra viruslar turlari?

a) Shifrlangan, shifrlanmagan, polimorf   
b) Dasturiy, yuklanuvchi, makroviruslar, multiplatformali viruslar   
c) Rezident, norezident   
d) Virus parazit, virus cherv

175. Dasturiy shifrlash vositalari necha turga bo‘linadi?

a) 4   
b) 3   
c) 5   
d) 6

176. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ...

a) Krakker   
b) Hakker   
c) Virus bot   
d) Ishonchsiz dasturchi

177. DIR viruslari nimani zararlaydi?

a) FAT tarkibini zararlaydi   
b) com, exe kabi turli fayllarni zararlaydi   
c) yuklovchi dasturlarni zararlaydi   
d) Operatsion tizimdagi sonfig.sys faylni zararlaydi

178. Diskni shifrlash nima uchun amalga oshiriladi?

a) Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi   
b) Xabarni yashirish uchun amalga oshiriladi   
c) Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi   
d) Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi

179. Doktorlar, detektorlarga xos bo‘lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang.

a) Faglar   
b) Detektorlar   
c) Vaksinalar   
d) Privivka

180. Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi.

a) Fizik sath (physical)   
b) Kanal sath (data link)i   
c) Tarmoq sathi   
d) Transport sathi

181. Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?

a) raqamli imzoni shakllantirish va tekshirish muolajasi   
b) raqamli imzoni hisoblash muolajasi   
c) raqamli imzoni hisoblash va tekshirish muolajasi   
d) raqamli imzoni shakllantirish muolajasi

182. Eng ko‘p axborot xavfsizligini buzilish xolati-bu:

a) Tarmoqda ruxsatsiz ichki foydalanish   
b) Tizimni loyihalash xatolaridan foydalanish   
c) Tashqi tarmoq resursiga ulanish   
d) Simsiz tarmoqqa ulanish

183. Enterprise Information Security Policies, EISP-bu…

a) Tashkilot axborot xavfsizligi siyosati   
b) Muammofa qaratilgan xavfsizlik siyosati   
c) Tizimga qaratilgan xavfizlik siyosati   
d) Maqbul foydalanish siyosati

184. Ethernet konsentratori(hub) qanday vazifani bajaradi?

a) kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo‘naltirib beradi   
b) kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo‘naltirib beradi   
c) kompyuterdan kelayotgan axborotni xalqa bo‘ylab joylashgan keyingi kompyuterga   
d) tarmoqning ikki segmentini bir biriga ulaydi

185. Faol hujum turi deb nimaga aytiladi?

a) Maxfiy uzatish jarayonini uzib qo‘yish, modifikatsiyalash, qalbaki shifr ma’lumotlar tayyorlash harakatlaridan iborat jarayon   
b) Maxfiy ma’lumotni aloqa tarmog‘ida uzatilayotganda eshitish, tahrir qilish, yozib olish   
c) harakatlaridan iborat uzatilalayotgan ma’lumotni qabul qiluvchiga o‘zgartirishsiz yetkazish jarayoni   
d) Ma’lumotga o‘zgartirish kiritmay uni kuzatish jarayoni   
e) Sust hujumdan farq qilmaydigan jarayon

186. Faollashish prinspiga ko‘ra viruslar turlari?

a) Rezident, Norezident   
b) Dasturiy, Makroviruslar, multiplatformali viruslar   
c) Virus parazit, Virus cherv   
d) Shifrlangan, shifrlanmagan, Polimorf

187. Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o‘zgarib turadigan parol nima deyiladi?

a) One-time password (OTP)   
b) Only password (OP)   
c) First Password (FP)   
d) Primary Password (PP)

188. Faqat ma’lum hizmatlar /hujumlar/harakatlar bloklanadi. Bu qaysi xavfsizlik siyosatiga hos?

a) Ruxsat berishga asoslangan siyosat (Permissive Policy)   
b) Ehtiyotkorlik siyosati (Prudent Policy)   
c) Nomuntazam siyosat (Promiscuous Policy)   
d) Paranoid siyosati (Paranoid Policy)

189. Fire Wall ning vazifasi...

a) Tarmoqlar orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta`minlaydi   
b) kompyuterlar tizimi xavfsizligini ta`minlaydi   
c) Ikkita kompyuter o‘rtasida aloqa o‘rnatish jarayonida Internet tarmog‘i orasida xavfsizlikni ta`minlaydi   
d) uy tarmog‘i orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta`minlaydi

190. Fizik to‘siqlarni o‘rnatish , Xavfsizlik qo‘riqchilarini ishga olish, Fizik qulflar qo‘yishni amalga oshirish qanday nazorat turiga kiradi?

a) Fizik nazorat   
b) Texnik nazorat   
c) Ma’muriy nazorat   
d) Tashkiliy nazorat

191. Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi?

a) 2 taga   
b) 4 taga   
c) 3 taga   
d) 5 taga

192. Fizik xavfsizlikni nazoratlashga nimalar kiradi?

a) Binoga to‘siqlar qo‘yish, eshikka qulflar o‘rnatish, xavfsizlik xodimlarini ishga olish.   
b) Kompyuterlarga antivirus o‘rnatish, serverlarni ko‘paytirish, to‘siqlarni o‘rnatish   
c) Hujjatlarni tashkillashtirish, xodimlarni o‘qitish,qulflarni o‘rnatish   
d) Ruxsatni nazoratlash,shaxs xavfsizligini ta’minlash,muhitni nazoratlash

193. Foydalanish huquqini cheklovchi matritsa modeli bu...

a) Bella La-Padulla modeli   
b) Dening modeli   
c) Landver modeli   
d) Huquqlarni cheklovchi model

194. Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari-bu…

a) Foydalanuvchanligi   
b) Ma’lumotlar butunligi   
c) Axborotning konfedensialligi   
d) Ixchamligi

195. Foydalanishda boshqarishda ma’lumot , resurs, jarayon nima deb ataladi?

a) Obyekt   
b) Subyekt   
c) Tizim   
d) Ruxsat

196. Foydalanishni boshqarish –bu...

a) Subyektni Obyektga ishlash qobilyatini aniqlashdir.   
b) Subyektni Subyektga ishlash qobilyatini aniqlashdir.   
c) Obyektni mizojga ishlash qobilyatini aniqlashdir   
d) Autentifikatsiyalash jarayonidir

197. Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar qanday vazifani bajaradi?

a) Subyekt   
b) Obyekt   
c) Tizim   
d) Ruxsat

198. Foydalanishni boshqarishda subyekt bu - ....

a) Inson, dastur, jarayon   
b) Jarayon, dastur   
c) Ma’lumot, resurs, jarayon   
d) Resurs

199. Foydalanishni boshqarishning asosan nechta bor?

a) 4   
b) 5   
c) 6   
d) 7

200. Foydalanishni boshqarishning ….. usuli tizimdagi shaxsiy obyektlarni himoyalash uchun qo‘llaniladi?

a) Discretionary access control( DAC)   
b) Mandatory access control (MAC)   
c) Role-based access control (RBAC)   
d) Attribute based access control (ABAC)

201. Foydalanishni boshqarishning ….usulida foydalanishlar subyektlar va obyektlarni klassifikatsiyalashga asosan boshqariladi.

a) Mandatory access control (MAC)   
b) Discretionary access control( DAC)   
c) Role-based access control (RBAC)   
d) Attribute based access control (ABAC)

202. Foydalanishni boshqarishning …. usulida ruxsatlar va xarakatni kim bajarayotganligi to‘g‘risidagi xolatlar “agar, u xolda” buyrug‘idan tashkil topgan qoidalarga asoslanadi.

a) Attribute based access control (ABAC)   
b) Discretionary access control( DAC)   
c) Mandatory access control (MAC)   
d) Role-based access control (RBAC)

203. Foydalanishni boshqarishning …. usulida subyekt va obyektlarga tegishli huquqlarni ma’murlash oson kechadi.

a) Role-based access control (RBAC)   
b) Discretionary access control( DAC)   
c) Mandatory access control (MAC)   
d) Attribute based access control (ABAC)

204. Foydalanishni boshqarishning …. usulida xavfsizlik markazlashgan tarzda xavfsizlik siyosati ma’muri tomonidan amalga oshiriladi.

a) Mandatory access control (MAC)   
b) Discretionary access control( DAC)   
c) Role-based access control (RBAC)   
d) Attribute based access control (ABAC)

205. Foydalanishni boshqarishning Discretionary access control( DAC) usulidan asosan ….. qo‘llaniladi.

a) Operatsion tizimlarda   
b) Ma’lumotlar bazasida   
c) Web saytlarda   
d) Kompyuter tarmoqlarda

206. Tarmoqda foydalanuvchilarga tegishli ma’lumotlarini qo‘lga kiritub, uni hujum qiluvchiga yuboraradigan dasturiy kod qanday ataladi?

a) Spyware   
b) Rootkits   
c) Backdoors   
d) Ransomware

207. Kompyuter tarmoqdagi foydalanuvchilar harakatini, uning axborot resurslardan foydalanishga urinishini qayd etish qansi atama bilan nomlanadi?

a) Ma’murlash   
b) Identifikatsiyalash   
c) Autentifikatsiyalash   
d) Aniqlash

208. Global tamoq dastlab paytda qaysi nom bilan atalgan?

a) ARPANET   
b) NETWORK   
c) INTRANET   
d) INTERNET

209. ….-mavjud tahdidni amalga oshirilgan ko‘rinishi bo‘lib, bunda kutilgan tahdid amalga oshiriladi.

a) Hujum   
b) Tahdid   
c) Zaiflik   
d) Buzish

210. Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilarga tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni – bu…

a) Avtorizatsiya   
b) Identifikatsiya   
c) Autentifikatsiya   
d) Ma’murlash

211. IEEE 802.11, Wi-Fi standartini qo‘llovchi tarmoq turini aniqlang.

a) Lokal simsiz tarmoq   
b) Shaxsiy simsiz tarmoq   
c) Regional simsiz tarmoq   
d) Global simsiz tarmoq

212. IEEE 802.16, WiMAX standartini qo‘llovchi tarmoq turini aniqlang.

a) Shahar simsiz tarmoq   
b) Shaxsiy simsiz tarmoq   
c) Lokal simsiz tarmoq   
d) Global simsiz tarmoq

213. Elektron imzoni haqiqiyligini tekshirish … amalga oshiriladi.

a) Imzo muallifining ochiq kaliti yordamida   
b) Ma’lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida   
c) Ma’lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida   
d) Imzo muallifining maxfiy kaliti yordamida

214. DoS hujumlari oqibati quyidagilardan qaysi biri sodir bo‘ladi?

a) Foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan mahrum qilinadilar   
b) Foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzg‘unchilarga etkaziladi   
c) Axborot tizimidagi ma’lumotlar bazalari o‘g‘irlanib ko‘lga kiritilgach, ular yo‘q qilinadilar   
d) Foydalanuvchilar axborotlariga ruxsatsiz o‘zgartirishlar kiritilib, ularning yaxlitligi buziladi

215. Kriptografiga “Kalit” atamasiga qanday ta’rif beriladi?

a) axborotni shifrlash va deshifrlash uchun kerakli axborot   
b) Bir qancha kalitlar yig‘indisi   
c) Axborotli kalitlar to‘plami   
d) Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

216. Kalitlar boshqaruvi qanday elementga ega bo‘ladi?

a) hosil qilish, yig‘ish, taqsimlash   
b) ishonchliligi, maxfiyligi, aniqligi   
c) xavfsizlik, tez ishlashi, to‘g‘ri taqsimlanishi   
d) abonentlar soni, xavfsizligi, maxfiyligi

217. Kiberxavfsizkda “tahdid” atamasi qanday ta’riflanadi?

a) Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa   
b) Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa   
c) Bu riskni o‘zgartiradigan harakatlar   
d) Bu noaniqlikning maqsadlarga ta’siri

218. Kiberxavfsizlik nechta bilim soxasini o‘z ichiga oladi?

a) 8 ta   
b) 6 ta   
c) 5 ta   
d) 7 ta

219. Kiberxavfsizlikni ta’minlash masalalari bo‘yicha xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang.

a) SANS (System Administration Networking and Security)   
b) Department of defence (DOD)   
c) Discretionary access control   
d) Attribute based access control

220. Kimlar o‘zining harakatlari bilan sanoat josusi yetkazadigan muammoga teng (undan ham ko‘p bo‘lishi mumkin) muammoni yuzaga keltiradi?

a) Ishonchsiz xodimlar   
b) Xaker-proffesional   
c) Sarguzasht qidiruvchilar   
d) G‘oyaviy xakerlar

221. Kompyuter bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning xatti-harakatlari, komyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko‘rsatishini o‘rgatadigan soha nima deb ataladi?

a) Kiberetika   
b) Kiberhuquq   
c) Kiberqoida   
d) Kiberxavfsizlik

222. Tarmoq qurilmalari IPv4 manzilni to‘g‘ri kiritilishini ko‘rsating.

a) 172.25.100.100   
b) 12:AC:14:1C:3B:13   
c) 255.255.255.0   
d) 1001000110111

223. Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi…

a) Kompyuter tarmoqlari   
b) Kompyuter markazi   
c) Ma’lumotlar bazasi   
d) Tarmoq xavfsizligi

224. ….kompyuter tizimiga tahdid qilish imkoniyatiga ega va troyanlar, viruslar, “qurt”lar ko‘rinishida bo‘lishi mumkin.

a) Zararli dastur   
b) .exe fayl   
c) Boshqariluvchi dastur   
d) Kengaytmaga ega bo‘lgan fayl

225. ….bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida o‘zini ko‘rsatsada, yashiringan zararli koddan iborat.

a) troyan otlari   
b) adware   
c) spyware   
d) rootkits

226. ….zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi.

a) mantiqiy bombalar   
b) adware   
c) spyware   
d) rootkits

227. ….keng qamrovli nishondagi tizim va tarmoq resurlarida xizmatdan foydalanishni buzishga qaratilgan hujum bo‘lib, Internetdagi ko‘plab zombi kompyuterlar orqali bilvosita amalga oshiriladi.

a) Taqsimlangan DOS hujumlar   
b) O‘rtada turgan odam hujumi   
c) Parolga qaratilgan hujumlar   
d) Passiv razvedka hujumlari

228. Qaysi hujumlar asosan portlarni va operaesion tizimni skanerlashni maqsad qiladi?

a) Aktiv razvedka hujumlari   
b) O‘rtada turgan odam hujumi   
c) Parolga qaratilgan hujumlar   
d) Passiv razvedka hujumlari

229. …. hujumlari trafik orqali axborotni to‘plashga harakat qiladi. Buning uchun hujumchi sniffer deb nomlanuvchi dasturiy vositadan foydalanadi.

a) Passiv razvedka hujumlari   
b) Aktiv razvedka hujumlari   
c) O‘rtada turgan odam hujumi   
d) Parolga qaratilgan hujumlar

230. …. nishondagi kompyuter tizimi uchun nazoratni qo‘lga kiritish yoki ruxsatsiz foydalanish maqsadida amalga oshiriladi.

a) Passiv razvedka hujumlari   
b) Aktiv razvedka hujumlari   
c) O‘rtada turgan odam hujumi   
**d) Parolga qaratilgan hujumlar**

231. … hujumda hujum qiluvchi o‘rnatilgan aloqaga suqilib kiradi va aloqani uzadi.

a) Passiv razvedka hujumlari   
b) Aktiv razvedka hujumlari   
**c) O‘rtada turgan odam hujumi**   
d) Parolga qaratilgan hujumlar

232. Konfidentsial axborotdan foydalanish tushunchasi…

a) Muayyan shaxsga tarkibida konfidensial xarakterli ma’lumot bo‘lgan axborot bilan tanishishga vakolatli mansabdor shaxsning ruxsati.   
b) Korxona o‘z faoliyatini buzilishsiz va to‘xtalishsiz yurgiza oladigan vaqt bo‘yicha barqaror bashoratlanuvchi atrof-muhit holati.   
c) Ma’lumotlarning ma’lumotlar bazasiga tegishli darajasini aniqlash va belgilash.   
d) Olingan ma’lumotlar jo‘natuvchisining so‘ralganiga mosligini tasdiqlash

233. Kriptoanaliz qanday jarayonlarni o‘rganadi?

a) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi   
b) axborotni qayta akslantirishning texnik usullarini izlaydi va tadqiq qiladi   
c) axborotni akslantirib himoyalash muammosi bilan shug‘ullanadi   
d) kalitni qo‘llab matnni ochish imkoniyatlarini o‘rganadi

234. Kriptografiya qanday jarayonlarni o‘rganadi?

a) axborotni akslantirish va qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi   
b) axborotni qayta akslantirib himoyalash muammosi bilan shug‘ullanadi   
c) kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi   
d) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

235. Kriptologiya nechta yo‘nalishga bo‘linadi?

a) 2 ta   
b) 3 ta   
c) 4 ta   
d) 5 ta

236. Kompyuter tarmoqlarda qo‘llanuvchi topologiya turi qaysi?

a) Yulduz, shina, xalqa   
b) Markaziy, tengma-teng, aralash   
c) To‘liq bog‘langan, shina, aylana   
d) Shina, optik, koaksial

237. Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish jarayoni qanday ataladi?

a) Autentifikatsiya   
b) Identifikatsiya   
c) Ma’murlash (accaunting)   
d) Avtorizatsiya

238. Qog‘oz ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi?

a) 4 xil   
b) 8 xil   
c) 7 xil   
d) 5 xil

239. Ma’lumotlarni zaxira nusxalash bu – …

a) Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni   
b) Axborotni turli dasturlar yordamida tiklash imkoniyati   
c) Ma’lumotlarni ishonchli o‘chirish imkoniyati   
d) Ma'lumotlar xavfsizligini ta'minlash uchun qo‘llaniladigan shifrlash jarayoni

240. Turli offis ilovalari – MS Word hujjati, MS Excel elektron jadvali kabi fayllarni qaysi virus turi zararlaydi?

a) Makroviruslar   
b) Troyanlar   
c) Botnetlar   
d) Mutantvirus

241. Ma'lumotlarni zahira nusxasini saqlovchi va qayta tikovchi dasturni belgilang.

a) Redo Backup and Recovery   
b) BestCrypt   
c) Cryptool 1.4   
d) Eset32

242. Nomuntazam siyosat (Promiscuous Policy) nima?

a) Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi   
b) Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi   
c) Hamma narsa taqiqlanadi   
d) Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

243. OSI modelining birinchi sathi nomini belgilang.

a) Fizik sath (physical)   
b) Ilova sath (application)   
c) Seans sath (session)   
d) Kanal sath (data link)

244. OSI modelining ikkinchi sathi nomini belgilang .

a) Kanal sath (data link)   
b) Fizik sath (physical)   
c) Ilova sath (application)   
d) Seans sath (session)

245. OSI modelining uchinchi sathi nomini belgilang .

a) Tarmoq(network)   
b) Fizik sath (physical)   
c) Ilova sath (application)   
d) Seans sath (session)

246. OSI modelining to‘rtinchi sathi nomini belgilang .

a) Transport (transport)   
b) Fizik sath (physical)   
c) Ilova sath (application)   
d) Taqdimot (presentation)

247. OSI modelining beshinchi sathi nomini belgilang.

a) Seans sath (session)   
b) Fizik sath (physical)   
c) Ilova sath (application)   
d) Seans sath (session)

248. OSI modelining oltinchi sathi nomini belgilang.

a) Taqdimot (presentation)   
b) Fizik sath (physical)   
c) Ilova sath (application)   
d) Tarmoq(network)

249. OSI modelining yettinchi sathi nomini belgilang

a) Ilova sath (application)   
b) Seans sath (session)   
c) Fizik sath (physical)   
d) Tarmoq(network)

250. OSI modelida nechta sathdan iborat?

a) 7 ta   
b) 4 ta   
c) 5 ta   
d) 3 ta

251. OSI modelining Ilova sath (application) sathida qanday protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket   
b) ASCII, EBCDIC, JPEG, MIDI   
c) TCP, UDP, SCTP   
d) IPv4, IPv6, IPsec, AppleTalk, ICMP

252. OSI modelining Taqdimot (presentation) sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket   
**b) ASCII, EBCDIC, JPEG, MIDI**   
c) TCP, UDP, SCTP   
d) IPv4, IPv6, IPsec, AppleTalk, ICMP

253. OSI modelining Transport sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket   
b) ASCII, EBCDIC, JPEG, MIDI   
**c) TCP, UDP, SCTP**   
d) IPv4, IPv6, IPsec, AppleTalk, ICMP

254. OSI modelining Tarmoq (network) sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket   
b) ASCII, EBCDIC, JPEG, MIDI   
c) TCP, UDP, SCTP   
**d) IPv4, IPv6, IPsec, AppleTalk, ICMP**

255. OSI modelining Kanal (data link) sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket   
b) ASCII, EBCDIC, JPEG, MIDI   
c) TCP, UDP, SCTP   
**d) PPP, IEEE 802.22, Ethernet, DSL, ARP**

256. OSI modelining Fizik (physical) sathida qanday tarmoq qurilmalari qo‘llaniladi?

a) Marshrutizator   
b) Ko‘prik   
c) Tarmoq adapter   
**d) Kontsentrator**

257. OSI modelining Kanal (data link) sathida qanday tarmoq qurilmalar qo‘llaniladi?

a) Marshrutizator   
b) Ko‘prik   
c) Tarmoq ekrani   
**d) Kommutator**

258. OSI modelining Tarmoq (network) sathida qanday tarmoq qurilmalar qo‘llaniladi?

**a) Marshrutizator**   
b) Ko‘prik   
c) Tarmoq ekrani   
d) Kommutator

259. OSI modelining Fizik (physical) sathida axborot tipi qanday nomlanadi?

**a) bit**   
b) kadr   
c) paket   
d) segmet

260. OSI modelining Kanal (data link) sathida axborot tipi qanday nomlanadi?

a) ma’lumot   
**b) bit/kadr**   
c) paket   
d) segmet/datagramma

261. OSI modelining Tarmoq (network) sathida axborot tipi qanday nomlanadi?

a) ma’lumot   
b) bit/kadr   
**c) paket**   
d) segmet/datagramma

262. OSI modelining Transport sathida axborot tipi qanday nomlanadi?

a) ma’lumot   
b) bit/kadr   
c) paket   
**d) segmet/datagramma**

263. Paranoid siyosati (Paranoid Policy) – bu ….

**a) Hamma narsa ta’qiqlanadi**   
b) Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi   
c) Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi   
d) Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

264. Polimorf viruslar tushunchasi to‘g‘ri ko‘rsating.

a) Viruslar turli ko‘rinishdagi shifrlangan viruslar bo‘lib, o‘zining ikkilik shaklini nusxadan-nusxaga o‘zgartirib boradi   
b) Odatda foyl tarkibida yashirinib tarqaydi   
c) o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dasturkodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi   
d) Viruslar yuklangan qattiq diskdagi, disketa yoki fleshkasektorlarida joylashgan kichik programmalarni zararlaydi yoki uni almashtiradi.

265. Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi?

a) Shaxsiy tarmoq   
b) Lokal   
c) Mintaqaviy   
d) Campus

266. Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi?

a) DNS tizimlari   
b) TCP/IP   
c) Ethernet   
d) Token ring

267. Qanday hujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi?

a) Razvedka hujumlari   
b) Kirish hujumlari   
c) DOS hujumlari   
d) Zararli hujumlar

268. Qanday hujumda hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi?

a) Kirish hujumlari   
b) Razvedka hujumlari   
c) DOS hujumlar   
d) Zararli hujumlar

269. Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi?

a) Tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi   
b) Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi   
c) Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.   
d) Potensial zaiflikni aniqlash imkoniyati yo‘qligi

270. Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi?

a) Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi   
b) Tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi   
c) Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.   
d) Potensial zaiflikni aniqlash imkoniyati yo‘qligi

271. Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi?

a) Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.   
b) Tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi   
c) Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi   
d) Potensial zaiflikni aniqlash imkoniyati yo‘qligi

272. Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.

a) Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.   
b) Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.   
c) Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi   
d) Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi

273. Quyidagilardan MAN (metropolitan area network) tarmoqqa berilgan ta’rifni belgilang.

a) Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi   
b) Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.   
c) Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.   
d) Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi

274. Kompyuter tarmoqlaridan “Umumiy shina” topologiyasi xususiyati qanday?

a) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi   
b) Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi   
c) Yuboriluvchi va qabul qilinuvchi ma’lumot token yordamida manziliga yetkaziladi   
d) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi

275. Kompyuter tarmoqlaridan “Yulduzsimon” topologiyasiga ta'rif bering.

a) Har bir kompyuterni markaziy konsentrator bilan ulash orqali tashkil etiladi   
b) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi   
c) Yuboriluvchi va qabul qilinuvchi ma’lumot token yordamida manziliga yetkaziladi   
d) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi

276. Kompyuter tarmoqlaridan “Xalqasimon” topologiyasiga ta'rif bering.

a) Har bir kompyuter boshqa ikkita kompyuter bilan ulangan va signal aylana bo‘yicha o‘tadi   
b) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi   
c) Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi   
d) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi

277. Quyidagilardan qaysi birida tarmoqning “Uyali mesh” topologiyasiga ta'rif berilgan?

a) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi   
b) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi   
c) Yuboriluvchi va qabul qilinuvchi ma’lumot Token yordamida manziliga yetkaziladi   
d) Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi

278. Aksariyat tashkilotlar muhim ma’lumotlarini qaysi texnologiyasi asosida zaxira nusxalashni amalga oshiradilar?

a) Random Array of Independent Disks(RAID)   
b) Virtual private network(VPN)   
c) Point to Point   
d) HyperText Transfer Protocol(HTTP)

279. Ransomware zararli dasturi axborotlarga qanday zarar keltiradi?

a) mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi.   
b) marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.   
c) foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.   
d) bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi.

280. Ma ’murlash usuli bo‘yicha tarmoqlar qanday turlarga bo‘linadi?

a) “Bir rangli” va “mijoz server” turlarga   
b) Server va kliyent turlarga   
c) Asosiy va qo‘shimcha turlar   
d) Korporativ va xalqaro turlarga

281. Rezident bo‘lmagan viruslar qachon xotirani zararlaydi?

a) Faqat faollashgan vaqtida   
b) Faqat o‘chirilganda   
c) Kompyuter yoqilganda   
d) Tarmoq orqali ma’lumot almashishda

282. Risk, tahdid, zaiflik va ta’sir tushunchalari o‘rtasida o‘zaro bog‘lanish qanday ifodalanadi?

a) RISK = Tahdid x Zaiflik x Ta’sir   
b) RISK = Tahdid +Zaiflik + Ta’sir   
c) RISK = Tahdid x (Zaiflik +Ta’sir)   
d) RISK = Tahdid -Zaiflik +Ta’sir

283. Risk darajasi tarmoqga (yoki tizimga) natijaviy ta’sirning bahosi bo‘lib, quyidagi tenglik bilan ifodalanadi:

a) Risk darajasi = natija \* ehtimollik   
b) Risk darajasi = natija +ehtimollik.   
c) Risk darajasi = natija /ehtimollik.   
d) Risk darajasi = natija - ehtimollik.

284. Samarali risklarni boshqarishning rejasi risklarni aniqlashni va baholashni kafolatli amalga oshirishda …. va qayta ko‘rib chiqishni talab etadi.

a) Risk monitoringi   
b) Riskni tahlillash   
c) Muvaffaqiyatli risklar   
d) Tanazzulga uchragan risklar

285. Risk darajalari nechta turga bo‘linadi?

a) 4 ta   
b) 3 ta   
c) 2 ta   
**d) 5 ta**

286. Risklarni boshqarish –bu…

a) Risklarni aniqlash, baholash, javob berish va bo‘lishi mumkin bo‘lgan ta’sirga tashkilot tomonidan javob berilishini amalga oshirish jarayoni   
b) Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta’siri va ehtimolini o‘lchashni ta’minlaydi.   
c) Aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni.   
d) Risk monitoringi yangi risklarni paydo bo‘lish imkoniyatini aniqlash

287. Risklarni boshqarish jarayoni quyidagi asosiy nechta bosqichga ajratiladi?

a) 4 ta   
b) 2 ta   
c) 5 ta   
d) 3 ta

288. …. tashkilotning risklarni boshqarish usuliga amalga oshirish tadbirlarini belgilaydi va tashkilotda axborot xavfsizligi va risklarni boshqarish bo‘yicha faoliyatni birlashtimvchi tarkibiy jarayonni ta’minlaydi.

a) Risklarni boshqarish freymworki   
b) Risk monitoringi   
c) Riskni tahlillash   
d) Muvaffaqiyatli risklar

289. Rootkitlar qanday zararli amallar bajaradi?

a) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi   
b) bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi   
c) o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi   
d) ararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

290. Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?

a) Fizik nazorat   
b) Huquqiy nazorat   
c) Ma’muriy nazorat   
d) Tashkiliy nazorat

291. Shifrlash nima?

a) ochiq matnni shifrmatnga o‘zgartirish jarayoni   
b) shifrmatnni ochiq matnga o‘zgartiruvchi teskari jarayoni   
c) kalitni bilmasdan turib shifrmatn bo‘yicha ochiq matnni tiklash jarayoni   
d) alfavit elementlaridan tartiblangan nabor

292. Kriptotizim bu-…

a) ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o‘zgartirishlar oilasi   
b) shifrmatnni ochiq matnga o‘zgartiruvchi teskari jarayoni   
c) kalitni bilmasdan turib shifrmatn bo‘yicha ochiq matnni tiklash jarayoni   
d) alfavit elementlaridan tartiblangan nabor

293. Simmetrik kriptotizimlarda ... .

a) shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi   
b) bir-biriga matematik usullar bilan bog‘langan ochiq va yopiq kalitlardan foydalaniladi   
c) axborot ochiq kalit yordamida shifrlanadi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi   
d) kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi

294. Simsiz tarmoqlarni kategoriyalarini to‘g‘ri ko‘rsating?

a) Simsiz shaxsiy tarmoq, simsiz lokal tarmoq, simsiz shahar tarmoq va simsiz global tarmoq   
b) Simsiz internet tarmoq va Simsiz telefon tarmoq, Simsiz shaxsiy tarmoq va Simsiz global tarmoq   
c) Simsiz internet tarmoq va uy simsiz tarmog‘i   
d) Simsiz chegaralanmagan tarmoq , simsiz kirish nuqtalari

295. Spyware-qanday zararli dastur?

a) tarmoqda foydalanuvchilarga tegishli ma’lumotlarini qo‘lga kiritub, uni hujum qiluvchiga yuboraradigan dasturiy kod   
b) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.   
c) internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi   
d) zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi

296. Subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim qilish jarayoni nima?

a) Identifikatsiya   
b) Autentifikatsiya   
c) Avtorizatsiya   
d) Ma’murlash

297. Kompyuter virusining birinchi ta’rifni kim bergan?

a) 1984 yili Fred Koen   
b) 1951 yil Jon fon Neumann   
c) 1981 yil Elik Cloner   
d) 1990 yil Bill Geyts

298. Kompyuter viruslari hayot davrining ikkita asosiy bosqichini toping.

a) Saqlanish va bajarilish   
b) Yaralish va yashash   
c) Tarqalish va zararlash   
d) Zararlash va yo‘q bo‘lish

299. Kompyuter viruslarining bajarilish davri, odatda, nechta bosqichni o‘z ichiga oladi?

a) 5 ta   
b) 2 ta   
c) 3 ta   
d) 4 ta

300. O‘z-o‘zidan tarqalish mexanizmi amalga oshiriluvchi, tizimga zarar keltirmaydi, faqat diskdagi bo‘sh xotirani sarflaydigan viruslar qanday viruslar deb ataladi?

a) Beziyon viruslar   
b) Xavfsiz viruslar   
c) Xavfli viruslar   
d) Juda xavfli viruslar

301. Tizimda mavjudligi turli taassurot (ovoz, video) bilan bog‘liq, bo‘sh xotirani kamaytirsada, dastur va ma’lumotlarga ziyon yetkazmaydigan viruslar qanday viruslar deb ataladi?

a) Xavfsiz viruslar   
b) Beziyon viruslar   
c) Xavfli viruslar   
d) Juda xavfli viruslar

302. Kompyuter ishlashida jiddiy nuqsonlarga sabab bo‘luvchi, natijada dastur va ma’lumotlar buzilishiga olib kelivchi viruslar qanday viruslar deb ataladi?

a) Xavfli viruslar   
b) Xavfsiz viruslar   
c) Beziyon viruslar   
d) Juda xavfli viruslar

303. PPP-kadrlarni tarmoq sathi paketlariga inkapsulyatsiyalovchi kanal sathining tunnel protokolini belgilang.

a) L2TP (Layer 2 Tunneling Protocol)   
b) IPSec (IP Security)   
c) PPTP (Point-to-Point Tunneling Protocol)   
d) SSH (Secure Shell)

304. “nuqta-nuqta” xilidagi kanal sathining tunnel protokolini belgilang.

a) IPSec (IP Security)   
b) PPTP (Point-to-Point Tunneling Protocol)   
c) SSH (Secure Shell)   
d) L2TP (Layer 2 Tunneling Protocol)

305. Tarmoqlararo ekran (firewall, brandmaver) –bu…

a) Trafikni filtrlash mexanizmiga asoslangan tarmoqdan foydalanishni cheklashning bazaviy vositasi   
b) Qurilma perimetrli himoyalash masalasining kompleks yechimi hisoblanadi   
c) Ma’lumotlarni inkapsulyatsiyalash mexanizmlari, hamda qo‘shimcha autentifikatsiya, shifrlash, yaxlitlikni nazoratlash

306. Kiruvchi ma’lumotning uzunligi o‘zgaruvchan, chiqishda esa o‘zgarmas uzunlikdagi qiymatni qaytaradigan jarayon qanday ataladi?

a) Xesh funksiya   
b) О‘rniga qoyish akslantirish   
c) O‘rin almashtirish akslantirishi   
d) Elektron raqamli imzo

307. Ochiq matn simvollari bir alfavitdan olinib, unga mos shifrmatn simvollari boshqa bir alfavitdan olinadigan jarayon nomini belgilang.

a) О‘rniga qoyish akslantirish   
b) Xesh funksiya   
c) O‘rin almashtirish akslantirishi   
d) Elektron raqamli imzo

308. Ochiq matnda ishtirok etgan simvollar shifrmatnda ham ishtirok etib, faqat ularning o‘rnii almashadigan jarayon nomini belgilang.

a) O‘rin almashtirish akslantirishi   
b) О‘rniga qoyish akslantirish   
c) Xesh funksiya   
d) Elektron raqamli imzo

309. …. ashkilotning va u bilan bog‘liq boshqa komponentlar va interfeyslarning istalgan axborot xavfsizligi tizimi xolatini tavsiflaydi.

a) Kiberxavfsizlik arxitekturasi   
b) Kiberxavfsizlik siyosati   
c) Simmetrik shiflash   
d) Elektron raqamli imzo

310. Fishing hujumi usullari to‘g‘ri ko‘rsatilgan qatorni belgilang: 1.Soxta havola; 2.soxta lotereya; 3.TV reklama; 4. Tekin dasturlar; 5.DOS hujum 6.Razvedka

a) 1,2,4   
b) 2,3,5   
c) 3,5,6   
d) 4,5,6

Xato   
Qaysi siyosat tizim resurslarini foydalanishda hech qanday cheklovlar qo‘ymaydi?

Paranoid siyosat   
Zаxirаlаshning qаndаy turlаri mаvjud?   
Ichki, tаshqi   
Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ... .   
Hakker   
Axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi nima deb ataladi?   
Axborot tizimlari   
Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?   
RAID 0   
Spam bilan kurashishning dasturiy uslubida nimalar ko‘zda tutiladi?   
Elektron pochta qutisiga kelib tushadigan spamlar me’yoriy xujjatlar asosida cheklanadi va bloklanadi   
Botnet-nima?   
zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish.   
Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi?   
RAID 5   
Zararli dasturlar qanday turlarga bo‘linadi?   
Tabiiy dasturlar va suniy dasturlar   
Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o‘z ichiga oladi?   
Davlat va nodavlat tashkilotlari me’yorlarni   
Ma’lumotlarni zaxira nusxalash bu – …   
Ma'lumotlar xavfsizligini ta'minlash uchun qo‘llaniladigan shifrlash jarayoni   
Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...   
Global tarmoqdan uzib qo‘yish   
Dаstlаbki virus nechаnchi yildа yarаtilgаn?   
1988   
System-Specific SecurityPolicies, SSSP-bu…   
Muammoga qaratilgan xavfsizlik siyosati   
Enterprise Information Security Policies, EISP-bu…   
Tizimga qaratilgan xavfizlik siyosati   
Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?   
"To‘liq zaxiralash"   
"To‘q sariq kitob"da xavfsizlik kriteriyalari qanday bo‘limlardan iborat?   
O‘ta maxfiy, maxfiy

TO’G’RILARI:

OSI modelida nechta tarmoq satxi bor ?   
J: 7   
OSI modelining birinchi satxi qanday nomlanadi   
J: Fizik satx   
OSI modelining ikkinchi satxi qanday nomlanadi   
J: Kanal satxi   
OSI modelining uchinchi satxi qanday nomlanadi   
J: Tarmoq satxi   
OSI modelining oltinchi satxi qanday nomlanadi   
J: Taqdimlash satxi   
OSI modelining yettinchi satxi qanday nomlanadi   
J: Amaliy satx   
OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi   
J: fizik, kanal va tarmoq satxlari   
OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi   
J: Marshrutizator   
OSI modelining fizik satxi qanday funktsiyalarni bajaradi   
J: Elektr signallarini uzatish va qabul qilish   
Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ?   
J: Obyekt    
Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?   
J: Subyekt   
Simmetrik kriptotizimlarda ... jumlani davom ettiring   
J: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi   
Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.   
J: 2 turga   
Axborotning eng kichik o’lchov birligi nima?   
J: bit   
Ko‘z pardasi, yuz tuzilishi, ovoz tembri-: bular autentifikatsiyaning qaysi faktoriga mos belgilar?   
J: Biometrik autentifikatsiya   
Kriptografiyaning asosiy maqsadi...   
J: maxfiylik, yaxlitlilikni ta`minlash   
Ro’yxatdan o’tish bu?   
foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni   
Qanday xujumda zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi?   
J: Zararli hujumlar   
Qanday xujumda hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi?   
J: Kirish hujumlari   
Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub   
J: Ethernet, FDDI   
Xesh-:funktsiyani natijasi …   
J: fiksirlangan uzunlikdagi xabar   
Ethernet kontsentratori qanday vazifani bajaradi   
J: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi   
Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?   
J: fleshka, CD va DVD disklar   
Faol hujum turi deb…   
J: Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon   
Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi.   
J: MAC   
Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo‘llaniladi   
J: DAC   
Foydalanishni boshqarishning qaysi modelida Obyekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi   
J: DACfInternetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?   
Foydalanishni boshqarishning qaysi usuli -: Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.   
J: ABAC   
Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun Obyektlardan foydalanish ruxsati ko‘rsatiladi?   
J: RBAC   
To’rtta bir-:biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub   
J: Xalqa Yulduz To’liq bog’lanishli Yacheykali   
Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi?   
J: DNS tizimlari, Razvedka hujumlari   
…… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.   
J: Kiberxavfsizlik   
Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?   
J: raqamli imzoni shakllantirish va tekshirish muolajasi   
Kriptologiya -:   
J: axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi   
Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?   
J: Deshifrlash   
Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.   
J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik   
Autentifikatsiya faktorlari nechta   
J: 3   
Kriptografiyada matn –   
J: alifbo elementlarining tartiblangan to’plami   
Konfidentsiallikga to’g’ri ta`rif keltiring.   
J: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;   
Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-:ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu?   
J: login   
Kriptoanaliz –   
J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi   
sifatlarga ega bo’lishi kerak?   
J: ishonchli, qimmatli va to’liq   
Shifrlash –   
J: akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi   
Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?   
J: simmetrik kriptosistemalar   
Foydalanishni boshqarish –bu...   
J: Subyektni Obyektga ishlash qobilyatini aniqlashdir.   
Kompyuterning tashqi interfeysi deganda nima tushuniladi?   
J: kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari   
Kodlash nima?   
J: Ma’lumotni osongina qaytarish uchun hammaga   
Tarmoq kartasi bu...   
J: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.   
Elektron raqamli imzo deb –   
J: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha   
Hab bu...   
J: ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.   
Switch bu...   
J: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.   
Axborot xavfsizligining asosiy maqsadlaridan biri-: bu…   
J: Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish   
Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-:ketligi (maxfiy so’z) – bu?   
J: parol   
Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?   
J: SMTP, POP yoki IMAR   
Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi?   
J: Tez, aniq va maxfiyligiga   
Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.   
J: Yozish   
Qanday xujumda hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi?   
J: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari   
Kalit – bu …   
J: Matnni shifrlash va shifrini ochish uchun kerakli axborot   
Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi   
J: Fizik satx   
Blokli shifrlash-:   
J: shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish   
Kriptobardoshlilik deb …   
J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi   
Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi   
J: Xesh funksiyalar   
Kriptografiya –   
J: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi   
Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub   
J: TCP,UDP   
Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu -:   
J: steganografiya   
Yaxlitlikni buzilishi bu -: …   
J: Soxtalashtirish va o’zgartirish   
Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?   
J: barchasi   
Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub   
J: Ethernet, FDDI   
Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?   
J: Foydalanishni boshqarish   
Tarmoq repiteri bu…   
J: Signalni tiklash yoki qaytarish uchun foydalaniladi.   
Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?   
J: Ochiq kalitli kriptotizimlarda bir-:biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi   
Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi   
J: O‘qish   
MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi   
J: xavfsizlik siyosati ma’muri   
Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?   
J: Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi   
Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi   
J: Tarmoq satxi   
Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bog‘liq..   
J: Tashkilotda Obyektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi   
Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi   
J: {d, n} – yopiq, {e, n} – ochiq;   
Diskni shifrlash nima uchun amalga oshiriladi?   
J: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi   
Tahdid nima?   
J: Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.   
Risk   
J: Potensial foyda yoki zarar   
barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi?   
J: Fizik satx   
Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...   
J: Avtorizatsiya   
Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.   
J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik   
Kompyuter tarmoqlari bu –   
J: Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan   
Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?   
J: raqamli imzoni shakllantirish va tekshirish muolajasi   
Kriptografiyada matn –   
J: alifbo elementlarining tartiblangan to’plami   
Autentifikatsiya jarayoni qanday jarayon?   
J: obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash   
Rol tushunchasiga ta’rif bering.   
J: Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin   
Avtorizatsiya jarayoni qanday jarayon?   
J: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni   
Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima   
J: Parol   
Elektron raqamli imzo deb –   
J: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha   
TCP/IP modelida nechta satx mavjud   
J: 4   
Kriptoanaliz –   
J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi   
Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi?   
J: Simmetrik va assimetrik   
Shifrlash nima?   
J: Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi   
Kriptografiyada alifbo –   
J: axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam   
Kripto tizimga qo’yiladigan umumiy talablardan biri   
J: shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak   
Simmetrik kriptotizmning uzluksiz tizimida …   
J: ochiq matnning har bir harfi va simvoli alohida shifrlanadi   
Axborot resursi – bu?   
J: axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi   
Stenografiya ma’nosi...   
J: sirli yozuv   
Identifikatsiya jarayoni qanday jarayon?   
J: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni   
Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.   
J: Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.   
2. Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq?   
J:simmetrik kriptotizimlar   
3. Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.   
J:Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.   
4. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?   
J: parol   
5. Rol tushunchasiga ta’rif bering.   
Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin   
6. Foydalanish huquqini cheklovchi matritsa modeli bu...   
J:Bella La-Padulla modeli   
8. Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?   
J: Deshifrlash   
9. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?   
J:Strukturalarni ruxsatsiz modifikatsiyalash   
10. Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi?   
J:Kriptobardoshlik   
11. Foydalanishni boshqarish –bu...   
J: Sub’ektni Ob’ektga ishlash qobilyatini aniqlashdir.   
12. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?   
J: Yulduz   
13. RSA algoritm qaysi yilda ishlab chiqilgan?   
J: 1977 yil   
14. Elektron xujjatlarni yo‘q qilish usullari qaysilar?   
J:Shredirlash, magnitsizlantirish, yanchish   
15. Kriptografiyada kalitning vazifasi nima?   
J: Matnni shifrlash va shifrini ochish uchun kerakli axborot   
16. WiMAX qanday simsiz tarmoq turiga kiradi?   
J: Regional   
17. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…   
J: login   
18. Stenografiya ma’nosi qanday?   
J: sirli yozuv   
19. Fire Wall ning vazifasi...   
J: Tarmoqlar orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta’minlaydi   
20. Yaxlitlikni buzilishi bu - …   
J: Soxtalashtirish va o‘zgartirish

1. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko‘rsating?

DDoS (Distributed Denial of Service) hujum

1. Rezident virus…

tezkor xotirada saqlanadi

1. Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyoti fanda qanday nomladi?

AKT xavfsizlik siyosati

1. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.

Recuva, R.saver

1. Zaiflik – bu…

tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

1. Axborot xavfsizligi timsollarini ko‘rsating.

Alisa, Bob, Eva

1. Kiberetika tushunchasi:

Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

1. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuni qachon kuchga kirgan?

1997 yil 24 aprel

1. DIR viruslari nimani zararlaydi?

FAT tarkibini zararlaydi

1. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

Detektorlar

1. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?

"Issiq zaxiralash"

1. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...

Tamoqlararo ekranlarning o‘rnatilishi

1. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan

1. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…

Kiberjinoyat deb ataladi

1. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud?

detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar

1. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?

Ruxsat berishga asoslangan siyosat

1. DIR viruslari nimani zararlaydi?

FAT tarkibini zararlaydi

1. Makroviruslar nimalarni zararlaydi?

Ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.

1. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.

HandyBakcup

1. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.

"Sovuq saxiralash"

1. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.

Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

1. Polimorf viruslar tushunchasi to‘g‘ri ko‘rsating.

Viruslar turli ko‘rinishdagi shifrlangan viruslar bo‘lib, o‘zining ikkilik shaklini nusxadan-nusxaga o‘zgartirib boradi

1. Fishing (ing. Phishing – baliq ovlash) bu…

Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

|  |  |  |
| --- | --- | --- |
|  | Xavfsizlikning asosiy yo’nalishlarini sanab o’ting. | Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik |
|  | Axborot xavfsizligining asosiy maqsadlaridan biri- bu… | Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish |
|  | Konfidentsiallikga to’g’ri ta`rif keltiring. | axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; |
|  | Yaxlitlikni buzilishi bu - … | Soxtalashtirish va o’zgartirish |
|  | ... axborotni himoyalash tizimi deyiladi. | Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi |
|  | Kompyuter virusi nima? | maxsus yozilgan va zararli dastur |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya mahnosi... | sirli yozuv |
|  | Kriptologiya yo’nalishlari nechta? | 2 |
|  | Kriptografiyaning asosiy maqsadi... | maxfiylik, yaxlitlilikni ta`minlash |
|  | SMTP - Simple Mail Transfer protokol nima? | elektron pochta protokoli |
|  | SKIP protokoli... | Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi |
|  | Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar… | uzilish, tutib qolish, o’zgartirish, soxtalashtirish |
|  | ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. | konfidentsiallik |
|  | Foydalanish huquqini cheklovchi matritsa modeli bu... | Bella La-Padulla modeli |
|  | Kommunikatsion qism tizimlarida xavfsizlikni ta`minlanishida necha xil shifrlash ishlatiladi? | 2 |
|  | Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? | TCP/IP, X.25 protokollar |
|  | Himoya tizimi kompleksligiga nimalar orqali erishiladi? | Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali |
|  | Kalit – bu … | Matnni shifrlash va shifrini ochish uchun kerakli axborot |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | simmetrik kriptotizimlar |
|  | Autentifikatsiya nima? | Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi |
|  | Identifikatsiya bu- … | Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni |
|  | O’rin almashtirish shifri bu - … | Murakkab bo’lmagan kriptografik akslantirish |
|  | Simmetrik kalitli shifrlash tizimi necha turga bo’linadi. | 2 turga |
|  | Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular … | hosil qilish, yig’ish, taqsimlash |
|  | Kriptologiya - | axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi |
|  | Kriptografiyada alifbo – | axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam |
|  | Simmetrik kriptotizimlarda ... jumlani davom ettiring | shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi |
|  | Kriptobardoshlilik deb … | kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Elektron raqamli imzo deb – | xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha |
|  | Kriptografiya – | axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi |
|  | Kriptografiyada matn – | alifbo elementlarining tartiblangan to’plami |
|  | Kriptoanaliz – | kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Shifrlash – | akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi |
|  | Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi? | Tez, aniq va maxfiyligiga |
|  | Faol hujum turi deb… | Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon |
|  | Blokli shifrlash- | shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish |
|  | Simmetrik kriptotizmning uzluksiz tizimida … | ochiq matnning har bir harfi va simvoli alohida shifrlanadi |
|  | Kripto tizimga qo’yiladigan umumiy talablardan biri | shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak |
|  | Quyidagi tengliklardan qaysilari shifrlash va deshifrlashni ifodalaydi? | Ek1(T)=T, Dk2(T1)=T |
|  | Berilgan ta`riflardan qaysi biri assimmetrik tizimlarga xos? | Assimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi |
|  | Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang | Vijiner matritsasi, Sezar usuli |
|  | Akslantirish tushunchasi deb nimaga aytiladi? | 1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga |
|  | Simmetrik guruh deb nimaga aytiladi? | O’rin almashtirish va joylashtirish |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | simmetrik kriptositemalar |
|  | Xavfli viruslar bu - … | kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Elektron raqamli imzo tizimi qanday muolajani amalga oshiradi? | raqamli imzoni shakllantirish va tekshirish muolajasi |
|  | Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? | Simmetrik va assimetrik |
|  | Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin? | Korporativ va umumfoydalanuvchi |
|  | Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo’linadi? | Sust va faol |
|  | Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? | SMTP, POP yoki IMAR |
|  | Axborot resursi – bu? | axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi |
|  | Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu? | login |
|  | Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu? | parol |
|  | Identifikatsiya jarayoni qanday jarayon? | axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni |
|  | Autentifikatsiya jarayoni qanday jarayon? | ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash |
|  | Avtorizatsiya jarayoni qanday jarayon? | foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni |
|  | Ro’yxatdan o’tish bu? | foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni |
|  | Axborot qanday sifatlarga ega bo’lishi kerak? | ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | bit |
|  | Elektronhujjatning rekvizitlari nechta qismdan iborat? | 4 |
|  | Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? | fleshka, CD va DVD disklar |
|  | Imzo bu nima ? | hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati. |
|  | Muhr bu nima? | hujjatning haqi-qiyligini va biror bir yuridik shaxsga tegishli ekanligi-ni tasdiqlovchi isbotdir. |
|  | DSA – nima | Raqamli imzo algoritmi |
|  | El Gamal algoritmi qanday algoritm | Shifrlash algoritmi va raqamli imzo algoritmi |
|  | Sezarning shifrlash sistemasining kamchiligi | Harflarning so’zlarda kelish chastotasini yashirmaydi |
|  | Axborot xavfsizligi va xavfsizlik san’ati haqidagi fan …. deyiladi? | Kriptografiya |
|  | Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu - | steganografiya |
|  | Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? | Deshifrlash |
|  | …… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. | Kiberxavfsizlik |
|  | Risk | Potensial foyda yoki zarar |
|  | Kiberxavfsizlik nechta bilim soxasini o‘z ichiga oladi. | 8 |
|  | “Ma’lumotlar xavfsizligi” bilim sohasi...... | ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi. |
|  | “Dasturiy ta’minotlar xavfsizligi” bilim sohasi..... | foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi. |
|  | “Tashkil etuvchilar xavfsizligi” ..... | katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi. |
|  | “Aloqa xavfsizligi” bilim sohasi...... | tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi. |
|  | “Tizim xavfsizligi” bilim sohasi…… | tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi. |
|  | “Inson xavfsizligi” bilim sohasi…. | kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi. |
|  | “Tashkilot xavfsizligi” bilim sohasi …. | tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini |
|  | “Jamoat xavfsizligi” bilim sohasi ….. | u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi. |
|  | Tahdid nima? tizim yoki | Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
|  | Kodlash nima? | Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir |
|  | Shifrlash nima? | Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi |
|  | Bir martalik bloknotda Qanday kalitlardan foydalaniladi? | Ochiq kalitdan |
|  | Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing. | 23 |
|  | Agar RSA algotirmida n ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi. | M = Cd mod n; |
|  | O’nlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq tizi miga o’tkazing. 65 | 100001 |
|  | Quyidagi modulli ifodani qiymatini toping. (125\*45)mod10. | 5 |
|  | Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256. | 244 |
|  | Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi. | C = Me mod n; -tog’ri javob |
|  | Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi | Kriptologiya. |
|  | Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi | {*d, n*} – yopiq, {*e, n*} – ochiq; |
|  | Zamonaviy kriptografiya qanday bo’limlardan iborat? | Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish |
|  | 1. Kriptografik usullardan foydalanishning asosiy yo’nalishlari nimalardan iborat? | Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarni haqiqiyligini aniqlash, tashuvchilarda axborotlarni shifrlangan ko’rinishda saqlash (masalan, hujjatlarni, ma’lumotlar bazasini) |
|  | Shifr nima? | Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm |
|  | Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? | Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi |
|  | Oqimli shifrlashning mohiyati nimada? | Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur, Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi |
|  | Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating. | uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim, |
|  | Kriptotizim quyidagi komponentlardan iborat: | ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, Ek : M ® C (shifrlash uchun) va Dk: C®M (deshifrlash uchun) funktsiyalar |
|  | Serpent, Square, Twofish, RC6 , AES algoritmlari qaysi turiga mansub? | simmetrik blokli algoritmlar |
|  | DES algoritmiga muqobil bo’lgan algoritmni ko’rsating. | Uch karrali DES, IDEA, Rijndael |
|  | DES algoritmining asosiy muammosi nimada? | kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas |
|  | Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? | shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun |
|  | 12+22 mod 32 ? | 2 |
|  | 2+5 mod32 ? | 7 |
|  | Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi. | ochiq kalitlar |
|  | 12+11 mod 16 ? | 7 |
|  | RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo’llab quvvatlaydi. | 128 bitli, 192 bitli, 256 bitli |
|  | Xesh-funktsiyani natijasi … | uzunlikdagi xabar |
|  | RSA algoritmi qanday jarayonlardan tashkil topgan | Kalitni generatsiyalash; Shifrlash; Deshifrlash. |
|  | RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida necha bit bo‘lishi talab etiladi. | 2048 |
|  | Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi | Xesh funksiyalar |
|  | To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub | Xalqa |
|  | Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo’llamasligi mumkin | to’liq bog’lanishli |
|  | Kompyuterning tashqi interfeysi deganda nima tushuniladi | kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari |
|  | Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi | Yulduz |
|  | Ethernet kontsentratori qanday vazifani bajaradi | kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi |
|  | OSI modelida nechta sath mavjud | 7 |
|  | OSI modelining to’rtinchi sathi qanday nomlanadi | Transport sathi |
|  | OSI modelining beshinchi sathi qanday nomlanadi | Seanslar sathi |
|  | OSI modelining birinchi sathi qanday nomlanadi | Fizik sath |
|  | OSI modelining ikkinchi sathi qanday nomlanadi | Kanal sathi |
|  | OSI modelining uchinchi sathi qanday nomlanadi | Tarmoq sathi |
|  | OSI modelining oltinchi sathi qanday nomlanadi | Taqdimlash sathi |
|  | OSI modelining ettinchi sathi qanday nomlanadi | Amaliy sath |
|  | OSI modelining qaysi sathlari tarmoqqa bog’liq sathlar hisoblanadi | fizik, kanal va tarmoq sathlari |
|  | OSI modelining tarmoq sathi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi | Marshrutizator |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi | Fizik sath |
|  | Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi sathi bajaradi | Tarmoq sathi |
|  | Keltirilgan protokollarning qaysilari tarmoq sathi protokollariga mansub | IP, IPX |
|  | Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub | TCP,UDP |
|  | OSI modelining fizik sathi qanday funktsiyalarni bajaradi | Elektr signallarini uzatish va qabul qilish |
|  | OSI modeliningamaliy sathi qanday funktsiyalarni bajaradi | Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | Keltirilgan protokollarning qaysilari kanal sathi protokollariga mansub | Ethernet, FDDI |
|  | Keltirilgan protokollarning qaysilari taqdimlash sathi protokollariga mansub | SNMP, Telnet |
|  | Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu... | Avtorizatsiya |
|  | Autentifikatsiya faktorlari nechta | 3 |
|  | Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima | Parol |
|  | Ko‘z pardasi, yuz tuzilishi, ovoz tembri. | Biometrik autentifikatsiya |
|  | barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi. | Fizik satx |
|  | Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi | 2 |
|  | Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi. | Foydalanishni boshqarish |
|  | Foydalanishni boshqarish –bu... | sub’ektni sub’ektga ishlash qobilyatini aniqlashdir. |
|  | Foydalanishna boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi, | Sub’ekt |
|  | Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ? | Ob’ekt |
|  | Foydalanishna boshqarishning nechta usuli mavjud? | 4 |
|  | Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy ob’ektlarni himoyalash uchun qo‘llaniladi | DAC |
|  | Foydalanishni boshqarishning qaysi modelida ob’ekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi | DAC |
|  | Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi. | MAC |
|  | Foydalanishni boshqarishning mandatli modelida Ob’ektning xavfsizlik darajasi nimaga bog‘liq.. | Tashkilotda ob’ektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi |
|  | MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi | xavfsizlik siyosati ma’muri |
|  | Agar sub’ektning xavfsizlik darajasida ob’ektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi | O‘qish |
|  | Agar sub’ektning xavfsizlik darajasi ob’ektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi. | Yozish |
|  | Foydalanishni boshqarishning qaysi modelida har bir ob’ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun ob’ektlardan foydalanish ruxsati ko‘rsatiladi? | RBAC |
|  | Rol tushunchasiga ta’rif bering. | Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin |
|  | Foydalanishni boshqarishning qaysi usuli - ob’ektlar va sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. | ABAC |
|  | XACML foydalanishni boshqarishni qaysi usulining standarti? | ABAC |
|  | Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan? | barchasi |
|  | Axborotning kriptografik himoya vositalari necha turda? | 3 |
|  | Dasturiy shifrlash vositalari necha turga bo‘linadi | 4 |
|  | Diskni shifrlash nima uchun amalga oshiriladi? | Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi |
|  | Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi? | 4 |
|  | Kompyuter tarmoqlari bu – | Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi |
|  | Tarmoq modeli –bu.. ikki | Hisoblash tizimlariorasidagi aloqani ularning ichki tuzilmaviy vatexnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir to‘plami |
|  | OSI modelida nechta tarmoq sathi bor | 7 |
|  | OSI modeli 7 stahi bu | Ilova |
|  | OSI modeli 1 stahi bu | Fizik |
|  | OSI modeli 2 stahi bu | Kanal |
|  | TCP/IP modelida nechta satx mavjud | 4 |
|  | Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi. | Shaxsiy tarmoq |
|  | Tarmoq kartasi bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Switch bu... | Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi |
|  | Hab bu... | ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. |
|  | Tarmoq repiteri bu... | Signalni tiklash yoki qaytarish uchun foydalaniladi. |
|  | Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi. | DNS tizimlari |
|  | ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. | TCP |
|  | …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi. | UDP |
|  | Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi. | IP |
|  | Tarmoq taxdidlari necha turga bo‘linadi | 4 |
|  | Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; | Razvedka hujumlari |
|  | Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi | Kirish hujumlari |
|  | Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi; | Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari |
|  | Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi; | Zararli hujumlar |
|  | Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? | Imzo qo‘yish va imzoni tekshirishdan |
|  | Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? | Imzo muallifining ochiq *kaliti yordamida* |
|  | Tarmoq modeli-bu... | Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir |
|  | OSI modeli nechta sathga ajraladi? | 7 |
|  | Fizik sathning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | Ilova sathning vazifasi nimadan iborat | Ilovalarni tarmoqqa ulanish jarayoni |
|  | Kanal sathning vazifasi nimadan iborat | Fizik manzillash |
|  | Tarmoq sathning vazifasi nimadan iborat | Yo‘lni aniqlash va mantiqiy manzillash |
|  | TCP/IP modeli nechta sathdan iborat | 4 |
|  | Quyidagilarninf qaysi biri Kanal sathi protokollari | Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri tarmoq sathi protokollari | . IP, ICMP, ARP, RARP |
|  | Quyidagilarninf qaysi biri transport sathi protokollari | TCP, UDP, RTP |
|  | Quyidagilarninf qaysi biri ilova sathi protokollari | HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP va hak |
|  | TCP/IP modelining kanal sathiga OSI modelining qaysi sathlari mos keladi | Kanal, Fizik |
|  | TCP/IP modelining tarmoq sathiga OSI modelining qaysi sathlari mos keladi | Tarmoq |
|  | TCP/IP modelining transport sathiga OSI modelining qaysi sathlari mos keladi | Tramsport |
|  | TCP/IP modelining ilova sathiga OSI modelining qaysi sathlari mos keladi | Ilova, taqdimot, seans |
|  | Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang. | . Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi. |
|  | Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang. | Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi |
|  | Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang. | Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi |
|  | Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan | Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi |
|  | Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan | Yuboriluvchi va qabul qilinuvchi ma’lumot TOKYeN yordamida manziliga yetkaziladi |
|  | Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan | Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi |
|  | Tarmoq kartasi nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Repetir nima? | Odatda signalni tiklash yoki qaytarish uchun foydalaniladi |
|  | Hub nima? | Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi |
|  | Switch nima? | Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi |
|  | Router nima? | Qabul qilingan ma’lumotlarni tarmoq sathiga tegishli manzillarga ko‘ra (IP manzil) uzatadi |
|  | DNS tizimlari. | Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi |
|  | TCP bu- … | Transmission Control Protocol |
|  | UDP bu-… | User datagram protocol |
|  | Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang | Ichki, tashqi |
|  | Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi | Biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi | Hujum natijasida ishlab chiqarishi yo‘qolgan hollarda uni qayta tiklash ko‘p vaqt talab qiladi va bu vaqtda ishlab chiqarish to‘xtab qoladi |
|  | Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi | Konfidensial axborotni chiqib ketishi natijasida, tashkilot shaxsiy ma’lumotlarini yo‘qolishi mumkin |
|  | Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi | Tashkilot xodimlarining shaxsiy va ishga oid ma’ulmotlarini kutilmaganda oshkor bo‘lishi ushbu xodimlarga bevosita ta’sir qiladi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi | tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. | Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi. |
|  | Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi | Razvedka hujumlari |
|  | Ma’lumotlarni zaxira nusxalash bu – … | Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi |
|  | Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz | Zaxira nusxalash |
|  | Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi? | 5 |
|  | Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. | 4 |
|  | Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | RAID texnologiyasining transkripsiyasi qanday. | Random Array of Independent Disks |
|  | RAID texnologiyasida nechta satx mavjud | 6 |
|  | OSI modelining birinchi sathi qanday nomlanadi | Fizik sath |
|  | OSI modelining ikkinchi sathi qanday nomlanadi | Kanal sathi |
|  | OSI modelining uchinchi sathi qanday nomlanadi | Tarmoq sathi |
|  | OSI modelining oltinchi sathi qanday nomlanadi | Taqdimlash sathi |
|  | OSI modelining ettinchi sathi qanday nomlanadi | Amaliy sath |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi | Fizik sath |
|  | Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub | TCP,UDP |
|  | OSI modelining fizik sathi qanday funktsiyalarni bajaradi | Elektr signallarini uzatish va qabul qilish |
|  | OSI modelining amaliy sathi qanday funktsiyalarni bajaradi | Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | 12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan sonlar soni nechta? | 8 ta |
|  | Yevklid algoritmi qanday natijani beradi? | Sonning eng katta umumiy bo’luvchisini toppish |
|  | Qanday sonlar tub sonlar deb yuritiladi? | Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi. |
|  | To‘liq zaxiralash | To‘liq va o‘sib boruvchi usullarning mujassamlashgan ko‘rinishi bo‘lib, oxirgi zaxiralangan nusxadan boshlab bo‘lgan o‘zgarishlarni zaxira nusxalab boradi. • Amalga oshirish to‘liq zaxiralashga qaraganda tez amalga oshiriladi. • Qayta tiklash o‘sib boruvchi zaxiralashga qaraganda tez amalga oshiriladi. • Ma’lumotni saqlash uchun to‘liq zaxiralashga qaraganda kam joy talab etadi |
|  | O‘sib boruvchi zaxiralash | Zaxiralangan ma’lumotga nisbatan o‘zgarish yuz berganda zaxirilash amalga oshiriladi. • Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usuli bo‘lishi mumkin (to‘liq saxiralashdan). • Saqlash uchun kam hajm va amalga oshirish jarayoni tez |
|  | Differensial zaxiralash | Ushbu zaxiralashda tarmoqga bog‘lanishamalga oshiriladi. • Iliq zaxiralashda, tizim yangilanishi davomiy yangilanishni qabul qilish uchun ulanadi |
|  | Ushbu jarayon ma’lumot qanday yo‘qolgani, ma’lumotni qayta tiklash dasturiy vositasi va ma’lumotni tiklash manzilini qayergaligiga bog‘liq bo‘ladi. Qaysi jarayon | Ma’lumotlarni qayta tiklash |
|  | Antivirus dasturlarini ko’rsating? | Drweb, Nod32, Kaspersky |
|  | Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi | wep, wpa, wpa2 |
|  | Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak? | ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | bit |
|  | Virtual xususiy tarmoq – bu? | VPN |
|  | Xavfli viruslar bu - … | kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Rezident virus... | tezkor xotirada saqlanadi |
|  | DIR viruslari nimani zararlaydi? | FAT tarkibini zararlaydi |
|  | .... kompyuter tarmoqlari bo’yicha tarqalib, komlg’yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi | «Chuvalchang» va replikatorli virus |
|  | Mutant virus... | shifrlash va deshifrlash algoritmlaridan iborat- to’g’ri javob |
|  | Fire Wall ning vazifasi... | tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi |
|  | Kompyuter virusi nima? | maxsus yozilgan va zararli dastur |
|  | Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating | disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali |
|  | Troyan dasturlari bu... | virus dasturlar |
|  | Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? | 5 |
|  | Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud | detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya mahnosi... | sirli yozuv |
|  | …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi | K.Shennon |
|  | Kriptologiya yo’nalishlari nechta? | 2 |
|  | Kriptografiyaning asosiy maqsadi... | maxfiylik, yaxlitlilikni ta`minlash |
|  | Zararli dasturiy vositalarni aniqlash turlari nechta | 3 |
|  | Signaiurana asoslangan | ...bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
|  | O‘zgarishni aniqlashga asoslangan | Zararli dasturlar biror joyda joylashishi sababli, agar tizimdagi biror joyga o‘zgarishni aniqlansa, u holda u zararlanishni ko‘rsatishi mumkin |
|  | Anomaliyaga asoslangan | Noodatiy yoki virusga o‘xshash yoki potensial zararli harakatlari yoki xususiyatlarni topishni maqsad qiladi |
|  | Antiairuslar qanday usulda viruslarni aniqlaydi | Signaturaga asoslangan |
|  | Viruslar - | o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi |
|  | Rootkitlar- | ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi |
|  | Backdoorlar - | zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish |
|  | Troyan otlari- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Ransomware- | mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi |
|  | Resurslardan foydalanish usuliga ko’ra viruslar qanday turlarga bo’linadi | Virus parazit, Virus cherv |
|  | Zararlagan obyektlar turiga ko’ra | Dasturiy, yuklanuvchi, Makroviruslar, multiplatformali viruslar |
|  | Faollashish prinspiga ko’ra | Resident, Norezident |
|  | Dastur kodini tashkil qilish yondashuviga ko‘ra | Shifrlangan, shifrlanmagan, Polimorf |
|  | Shifrlanmagan viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang | 840 |
|  | 256mod25=? | 6 |
|  | bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi. | Tizim |
|  | Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima duyidadi | Xavfsizlik siyosati |
|  | RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday? |  |

|  |  |  |
| --- | --- | --- |
| *p* va *q* –sonlarning ko‘paytmasini ifodalovchi sonning spektoriga teng; | DES algoritmi akslantirishlari raundlari soni qancha? | 16; |
|  | DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha? | CHap qism blok 32 bit, o‘ng qism blok 32 bit; |
|  | Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? | SHifrlash va deshifrlash jarayonlari uchun kalitlarni generatsiya qilish qoidalariga ko‘ra farqlanadi |
|  | 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta? | 18 ta |
|  | 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta? | 4 ta |
|  | Eyler funsiyasida 𝜙(1) qiymati nimaga teng? | 0 |
|  | Eyler funksiyasida 60 sonining qiymatini toping. | 59 |
|  | Eyler funksiyasi yordamida 1811 sonining qiymatini toping. | 1810 |
|  | 97 tub sonmi? | Tub |
|  | Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256. | 244 |
|  | Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220 | 44 |
|  | Quyidagi ifodani qiymatini toping. -17mod11 | 5 |
|  | 2 soniga 10 modul bo’yicha teskari sonni toping. | Ø |
|  | Tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta’minlash sohasidagi tadbirlar tavsiflanadigan yuqori darajadagi reja nima? | Kiberxavfsizlik siyosati |
|  | Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi? | tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi |
|  | Kiberxavfsizlikni ta’minlash masalalari bo’yicha xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang | SANS (System Administration Networking and Security) |
|  | Korxonaning davomli muvaffaqiyat bilan faoliyat yuritishinita’minlashga mo’ljallangan strukturalangan va o’zaro bog’langan harakatlar to’plami- … | Strategiya |
|  | Tahdidlarning muvaffaqiyatli amalga oshirilishiga imkon beruvchi har qanday omil – bu … | Zaiflik |
|  | ISO/IEC 27002:2005 – …. | Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari |
|  | O’zDStISO/IEC 27005:2013 – …. | Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish |
|  | Axborot xavfsizligi arxitekturasining nechta satxi bor? | 3 |
|  | Rahbariy hujjat. Ma’lumotlar uzatish tarmog’ida axborot xavfsizligini ta’minlash to’g’risida Nizom - Xujjat raqamini toping | RH 45-215:2009 |
|  | Davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta’minlash dasturini ishlab chiqish tartibi - Xujjat raqamini toping | RH 45-185:2011 |
|  | Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta’minlash darajasini aniqlash tartibi - Xujjat raqamini toping | RH 45-193:2007 |
|  | Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta’riflar - Xujjat raqamini toping | TSt 45-010:2010 |
|  | Quyidagilardan qaysi standart aloqa va axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta’riflarni belgilaydi? | TSt 45-010:2010 |
|  | Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni nima? | Identifikatsiya |
|  | Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima? | Autentifikatsiya |
|  | Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni – nima deyiladi? | Avtorizatsiya |
|  | Identifikatsiya nima? | Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni |
|  | Autentifikatsiya nima? | Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni |
|  | Avtorizatsiya nima? | Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni |
|  | ... - Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o’tishni ta’minlovchi biror axborot | Parol |
|  | Smart karta o’lchamidagi, kichik xajmdagi xotira va xisoblash imkoniyatiga ega bo’lgan, o’zida parol yoki kalitni saqlovchi qurilma nima deb ataladi? | Token, Smartkarta |
|  | Smarkarta nima asosida autentifikatsiyalaydi? | Something you have |
|  | Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o’zgarib turadigan parol nima deyiladi? | One-time password (OTP) |
|  | Foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish nima deb ataladi? | Ma’murlash |
|  | Amaldagi qonunchilikka mos ravishda texnik, dasturiy va dasturiy-texnik vositalar yordamida axborot xavfsizligining nokriptografik usullari bilan ta’minlashni inobatga oluvchi axborot himoyasi nima? | Axborotning texnik himoyasi |
|  | Nazorat hududi – bu ... | Qo’riqlanuvchi soha bo’lib, uning ichida kommunikatsiya qurilmalari hamda axborot tarmog’ining lokal tarkibiy qurilmalarini birlashtiruvchi barcha nuqtalar joylashadi |
|  | Texnik himoya vositalari – bu ... | Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob’ektni himoyalashdir |
|  | Bu axborotni tutib olish qurilmasi bo’lib, ularda uzatuvchi qurilma sifatida kontaktli mikrofonlardan foydalaniladi | Stetoskoplar |
|  | Xesh funktsiya to’g’ri ko’rsatilgan javobni aniqlang. | MD5 |
|  | MD5, SHA1, Tiger xesh funktsiyalari uchun blok uzunligi necha baytga teng? | 64 bayt |
|  | Sub’ektni ob’ektga ishlash qobilyatini aniqlash – nima? | Foydalanishni boshqarish |
|  | Foydalanishni boshqarishda sub’ekt bu - .... | Inson, dastur, jarayon |
|  | Foydalanishni boshqarishning qaysi usuli tizimdagi shaxsiy ob’ektlarni ximoyalash uchun qo’llaniladi? | Discretionary access control DAC |
|  | Foydalanishni boshqarishning qaysi usulidan asosan operatsion tizimlarda qo’llaniladi? | Discretionary access control DAC |
|  | Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi? | Mandatory access control MAC |
|  | Foydalanishni boshqarishning qaysi usulida xavfsizlik markazlashgan tarzda xavfsizlik siyosati m’muri tomonidan amalga oshiriladi? | Mandatory access control MAC |
|  | Foydalanishni boshqarishning qaysi usulida xar bir foydalanuvchini foydalanish ruxsatini belgilash o’rniga rol uchun ob’ektlardan foydalanish ruxsatini ko’rsatish yetarli bo’ladi? | Role-based access control RBAC |
|  | Foydalanishni boshqarishning qaysi usulida sub’ekt va ob’ektlarga tegishli xuquqlarni ma’murlash oson kechadi? | Role-based access control RBAC |
|  | Firibgarlikni oldini olish uchun bir shaxs tomonidan ko’plab vazifalarni bajarishga ruxsat bermaslik zarur. Bu muammo foydalanishni boshqarishni qaysi usulida bartaraf etiladi? | Role-based access control RBAC |
|  | Ob’ekt va sub’ektlarning attributlari, ular bilan mumkin bo’lgan amallar va so’rovlarga mos keladigan muxit uchun qoidalarni taxlil qilish asosida foydalanishni boshqarish - .... | Attribute based access control ABAC |
|  | Attribute based access control ABAC usuli attributlari qaysilar? | Foydalanuvchi attributlari, Resurs attributlari, Ob’ekt va muxit attributlari |
|  | Foydalanishni boshqarishning qaysi usulida ruxsatlar va xarakatni kim bajarayotganligi to’g’risidagi xolatlar “agar, u xolda” buyrug’idan tashkil topgan qoidalarga asoslanadi? | Attribute based access control ABAC |
|  | XASML standarti foydalanishni boshqarishning qaysi usulida qo’llaniladi? | Attribute based access control ABAC |
|  | XASML standartida qoida nima? | Maqsad, ta’sir, shart, majburiyat va maslaxatlar |
|  | XASML standartida maqsad nima? | Sub’ekt ob’ekt ustida nima xarakat qilishi |
|  | Lampsonning foydalanishni boshqarish matritsasi nimalardan tashkil topgan? | Imtiyozlar ro’yxati |
|  | Access control list va Capability list bu nimaning asosiy elementi xisoblanadi? | Lampson matritsasining |
|  | Lampson matritsasining satrlarida nima ifodalanadi? | Sub’ektlar |
|  | Foydalanishni boshqarishning mantiqiy vositalari infratuzilma va uning ichidagi tizimlarda ... uchun foydalaniladi. | Mandat, Tasdiqlash, Avtorizatsiya |
|  | SHaxsiy simsiz tarmoq standartini aniqlang. | Bluetooth, IEEE 802.15, IRDA |
|  | Lokal simsiz tarmoq standartini aniqlang. | IEEE 802.11, Wi-Fi, HiperLAN |
|  | Regional simsiz tarmoq standartini aniqlang. | IEEE 802.16, WiMAX |
|  | Global simsiz tarmoq standartini aniqlang. | CDPD, 2G, 2.5G, 3G, 4G, 5G |
|  | Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang. | SHaxsiy simsiz tarmoq |
|  | IEEE 802.11, Wi-Fi, HiperLAN standartida ishlovchi simsiz tarmoq turini aniqlang. | Lokal simsiz tarmoq |
|  | IEEE 802.16, WiMAX standartida ishlovchi simsiz tarmoq turini aniqlang. | Regional simsiz tarmoq |
|  | CDPD, 2G, 2.5G, 3G, 4G, 5G standartida ishlovchi simsiz tarmoq turini aniqlang. | Global simsiz tarmoq |
|  | Bluetooth qanday chastota oralig’ida ishlaydi? | 2.4-2.485 Ggts |
|  | Wi-Fi qanday chastota oralig’ida ishlaydi? | 2.4-5 Ggts |
|  | WiMax tarmog’ining tezligi qancha? | 1 Gbit/sekund |
|  | Quyidagilardan qaysi biri MITM xujumiga tegishli xatti-xarakat ximoblanadi? | Aloqa seansini konfidentsialligini va yaxlitligini buzish |
|  | WiMAX tarmoq arxitekturasi nechta tashkil etuvchidan iborat? | 5 |
|  | WiMAX tarmoq arxitekturasi qaysi tashkil etuvchidan iborat? | Base station, Subscriber station, Mobile station, Relay station, Operator network |
|  | GSM raqamli mobil telefonlarining nechanchi avlodi uchun ishlab chiqilgan protokol? | Ikkinchi avlodi |
|  | GSM standarti qaysi tashkilot tomonidan ishlab chiqilgan? | European telecommunications standards institute |
|  | .... – o’zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma’lumoti va xavfsizlik algoritmlarini saqlaydi. | Sim karta |
|  | Rutoken S qurilmasining og’irligi qancha? | 6.3 gramm |
|  | True Crypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES, Serpent, Twofish |
|  | Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidentsialligini aniqlash qaysi dasturiy shifrlash vositalarining vazifasi? | Disc encryption software |
|  | BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES, Serpent, Twofish |
|  | AxCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES-256 |
|  | Qog’oz ko’rinishidagi axborotlarni yo’q qilish qurilmasining nomini kiriting. | Shreder |
|  | Ma’lumotlarni bloklarga bo’lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya? | RAID 0 |
|  | Qaysi texnologiyada ma’lumotni ko’plab nusxalari bir vaqtda bir necha disklarga yoziladi? | RAID 1 |
|  | Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi? | RAID 3 |
|  | Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi? | RAID 5 |
|  | Disk zararlanganda “qaynoq almashtirish” yordamida uni almashtirish mumkin. Bu xususiyat qaysi texnologiyaga tegishli? | RAID 50 |
|  | Zaxiralashning qanday turlari mavjud? | To’liq, o’sib boruvchi, differentsial |
|  | IOS, Android, USB xotiralardan ma’lumotlarni tiklash uchun qaysi dasturdan foydalaniladi? | EASEUS Data recovery wizard |
|  | Foydalanuvchi ma’lumotlarini qo’lga kirituvchi va uni xujumchiga yuboruvchi dasturiy kod nima? | Spyware |
|  | Operatsion tizim tomonidan aniqlanmasligi uchun ma’lum xarakatlarni yashirish nima deyiladi? | Rootkits |
|  | Qurbon kompyuterda mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo’yib to’lov amalga oshirishni talab qiladi. Bu qaysi zararli dastur? | Ransomware |
|  | Quyidagilardan o’zidan ko’payishi yo’q bo’lganlarini belgilang. | Mantiqiy bomba, Troyan oti, Backdoors |
|  | Viruslar resurslardan foydalanish usuliga ko’ra qanday turlarga bo’linadi? | Virus parazitlar, virus chervlar |
|  | Viruslar zararlangan ob’ektlar turiga ko’ra qanday turlarga bo’linadi? | Dasturiy, yuklanuvchi, makroviruslar, ko’p platformali |
|  | Viruslar faollashish printsipiga ko’ra qanday turlarga bo’linadi? | Rezident, norezident |
|  | Viruslar dastur kodini tashkil qilish yondoshuviga ko’ra qanday turlarga bo’linadi? | SHifrlangan, shifrlanmagan, polimorf |
|  | Dastlabki virus nechanchi yilda yaratilgan? | 1988 |
|  | ILOVEYOU virusi keltirgan zarar qancha? | 10 mlrd. Dollar |
|  | CodeRed virusi keltirgan zarar qancha? | 2 mlrd. Dollar |
|  | Melissa virusi keltirgan zarar qancha? | 80 million dollar |
|  | NetSky virusi keltirgan zarar qancha? | 18 mlrd. Dollar |
|  | MyDoom virusi keltirgan zarar qancha? | 38 mlrd. Dollar |
|  | Risk monitoring ….. ni paydo bo’lish imkoniyatini aniqlaydi. | Yangi risklar |
|  | ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi. | Risk monitoring |
|  | Axborot xavfsizligi siyoatining necha hil turi bor? | 3 |
|  | Internetdan foydalanish siyosatining nechta turi mavjud? | 4 |
|  | Nomuntazam siyosat (Promiscuous Policy) nima? | Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi |
|  | Paranoid siyosati (Paranoid Policy) – bu …. | Hamma narsa ta’qiqlanadi |
|  | Ruxsat berishga asoslangan siyosat (Permissive Policy) – bu … | Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi |
|  | Ehtiyotkorlik siyosati (Prudent Policy) – bu …. | Barcha hizmatlar blokirovka qilingandan so’ng bog’lanadi |
|  | Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi. Bu qaysi xavfsizlik siyosatiga hos? | Nomuntazam siyosat (Promiscuous Policy) |
|  | Barcha hizmatlar blokirovka qilingandan so’ng bog’lanadi. Bu qaysi xavfsizlik siyosatiga hos? | Ehtiyotkorlik siyosati (Prudent Policy) |
|  | Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi. Bu qaysi xavfsizlik siyosatiga hos? | Ruxsat berishga asoslangan siyosat (Permissive Policy) |
|  | Hamma narsa ta’qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos? | Paranoid siyosati (Paranoid Policy) |
|  | Tizim arxitekturasining turlari nechta? | 5 |
|  | Internet, havo hujumidan mudofaa, transport tizimlari qaysi tizim arxitekturasiga xos? | Hamkorlik tizimlari arxitekturasi |
|  | Cloud computing texnologiyasining nechta asosiy turi mavjud? | 3 |
|  | Raqamli soatlar qaysi texnologiyaga tegishli? | O’rnatilgan tizimlar (Embedde systems) |
|  | Xavfsizlikning asosiy yo’nalishlarini sanab o’ting. | \*Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik |
|  | Axborot xavfsizligining asosiy maqsadlaridan biri- bu… | \*Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish |
|  | Konfidentsiallikga to’g’ri ta`rif keltiring. | \*axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; |
|  | Yaxlitlikni buzilishi bu - … | \*Soxtalashtirish va o’zgartirish |
|  | ... axborotni himoyalash tizimi deyiladi. | \*Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi |
|  | Kompyuter virusi nima? | \*maxsus yozilgan va zararli dastur |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | \*kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya ma’nosi... | \*sirli yozuv |
|  | Kriptografiyaning asosiy maqsadi... | \*maxfiylik, yaxlitlilikni ta`minlash |
|  | SMTP - Simple Mail Transfer protokol nima? | \*elektron pochta protokoli |
|  | SKIP protokoli... | \*Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi |
|  | Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar… | \*uzilish, tutib qolish, o’zgartirish, soxtalashtirish |
|  | ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. | \*konfidentsiallik |
|  | Foydalanish huquqini cheklovchi matritsa modeli bu... | \*Bella La-Padulla modeli |
|  | Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? | \*TCP/IP, X.25 protokollar |
|  | Himoya tizimi kompleksligiga nimalar orqali erishiladi? | \*Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali |
|  | Kalit – bu … | \*Matnni shifrlash va shifrini ochish uchun kerakli axborot |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | \*simmetrik kriptotizimlar |
|  | Autentifikatsiya nima? | \*Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi |
|  | Identifikatsiya bu- … | \*Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni |
|  | O’rin almashtirish shifri bu - … | \*Murakkab bo’lmagan kriptografik akslantirish |
|  | Simmetrik kalitli shifrlash tizimi necha turga bo’linadi. | \*2 turga |
|  | Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular … | \*hosil qilish, yig’ish, taqsimlash |
|  | Kriptologiya - | \*axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi |
|  | Kriptografiyada alifbo – | \*axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam |
|  | Simmetrik kriptotizimlarda ... jumlani davom ettiring | \*shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi |
|  | Kriptobardoshlilik deb … | \*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Elektron raqamli imzo deb – | \*xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha |
|  | Kriptografiya – | \*axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi |
|  | Kriptografiyada matn – | \*alifbo elementlarining tartiblangan to’plami |
|  | Kriptoanaliz – | \*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Shifrlash – | \*akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi |
|  | Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi? | \*Tez, aniq va maxfiyligiga |
|  | Faol hujum turi deb… | \*Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon |
|  | Blokli shifrlash- | \*shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish |
|  | Simmetrik kriptotizmning uzluksiz tizimida … | \*ochiq matnning har bir harfi va simvoli alohida shifrlanadi |
|  | Kripto tizimga qo’yiladigan umumiy talablardan biri | \*shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak |
|  | Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos? | \*Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi |
|  | Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang | \*Vijener matritsasi, Sezar usuli |
|  | Akslantirish tushunchasi deb nimaga aytiladi? | \*1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga |
|  | Simmetrik guruh deb nimaga aytiladi? | \*O’rin almashtirish va joylashtirish |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | \*simmetrik kriptosistemalar |
|  | Xavfli viruslar bu - … | \*kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | \*Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi? | \*raqamli imzoni shakllantirish va tekshirish muolajasi |
|  | Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? | \*Simmetrik va assimetrik |
|  | Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin? | \*Korporativ va umumfoydalanuvchi |
|  | Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo’linadi? | \*Sust va faol |
|  | Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? | \*SMTP, POP yoki IMAR |
|  | Axborot resursi – bu? | \*axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi |
|  | Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu? | \*login |
|  | Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu? | \*parol |
|  | Identifikatsiya jarayoni qanday jarayon? | \* axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni |
|  | Autentifikatsiya jarayoni qanday jarayon? | \*obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash |
|  | Avtorizatsiya jarayoni qanday jarayon? | \*foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni |
|  | Ro’yxatdan o’tish bu? | \*foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni |
|  | Axborot qanday sifatlarga ega bo’lishi kerak? | \*ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | \*bit |
|  | Elektron hujjatning rekvizitlari nechta qismdan iborat? | \*4 |
|  | Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? | \*fleshka, CD va DVD disklar |
|  | Imzo bu nima ? | \*hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati. |
|  | Muhr bu nima? | \*hujjatning haqiqiyligini va biror bir yuridik shaxsga tegishli ekanligini tasdiqlovchi isbotdir |
|  | DSA – nima | \*Raqamli imzo algoritmi |
|  | El Gamal algoritmi qanday algoritm | \*Shifrlash algoritmi va raqamli imzo algoritmi |
|  | Sezarning shifrlash sistemasining kamchiligi | \*Harflarning so’zlarda kelish chastotasini yashirmaydi |
|  | Axborot xavfsizligi va xavfsizlik san’ati haqidagi fan …. deyiladi? | \*Kriptografiya |
|  | Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu - | \*steganografiya |
|  | Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? | \*Deshifrlash |
|  | …… – hisoblashga asoslangan bilim sohasi bo‘lib,  buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. | \*Kiberxavfsizlik |
|  | Risk | \*Potensial foyda yoki zarar |
|  | Tahdid nima? | \*Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
|  | Kodlash nima? | \*Ma’lumotni osongina qaytarish uchun hammaga  ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir |
|  | Shifrlash nima? | Ma’lumotni osongina qaytarish uchun hammaga  ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir |
|  | Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi | Kriptoanaliz |
|  | Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi | {*d, e*} – ochiq, {*e, n*} – yopiq; |
|  | Zamonaviy kriptografiya qanday bo’limlardan iborat? | Electron raqamli imzo; kalitlarni boshqarish |
|  | Kriptografik usullardan foydalanishning asosiy yo’nalishlari nimalardan iborat? | uzatiliyotgan xabarlarni haqiqiyligini aniqlash |
|  | Shifr nima? | \* Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm |
|  | Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? | \*Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi |
|  | Oqimli shifrlashning mohiyati nimada? | Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,  Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi |
|  | Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating. | \*uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim, |
|  | Kriptotizim qaysi komponentlardan iborat? | \*ochiq matnlar fazosi M, Kalitlar fazosi K,  Shifrmatnlar fazosi C, Ek : M → C (shifrlash uchun) va Dk: C→M (deshifrlash uchun) funktsiyalar |
|  | Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? | \*shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun |
|  | Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi. | \*ochiq kalitlar |
|  | Xesh-funktsiyani natijasi … | Kiruvchi xabar uzunligidan uzun xabar |
|  | RSA algoritmi qanday jarayonlardan tashkil topgan | \*Kalitni generatsiyalash; Shifrlash; Deshifrlash. |
|  | Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi | \*Xesh funksiyalar |
|  | To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub | \*Xalqa |
|  | Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo’llamasligi mumkin? | \*to’liq bog’lanishli |
|  | Kompyuterning tashqi interfeysi deganda nima tushuniladi? | \*kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari |
|  | Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? | \*Yulduz |
|  | Ethernet kontsentratori qanday vazifani bajaradi | \*kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi |
|  | OSI modelida nechta satx mavjud | \*7 |
|  | OSI modelining to’rtinchi satxi qanday nomlanadi | \*Transport satxi |
|  | OSI modelining beshinchi satxi qanday nomlanadi | \*Seanslar satxi |
|  | OSI modelining birinchi satxi qanday nomlanadi | \*Fizik satx |
|  | OSI modelining ikkinchi satxi qanday nomlanadi | \*Kanal satxi |
|  | OSI modelining uchinchi satxi qanday nomlanadi | \*Tarmoq satxi |
|  | OSI modelining oltinchi satxi qanday nomlanadi | \*Taqdimlash satxi |
|  | OSI modelining yettinchi satxi qanday nomlanadi | \*Amaliy satx |
|  | OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi | \*fizik, kanal va tarmoq satxlari |
|  | OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi | \*Marshrutizator |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi | \*Fizik satx |
|  | Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi | \*Tarmoq satxi |
|  | Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub | \*IP, IPX |
|  | Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub | \*TCP,UDP |
|  | OSI modelining fizik satxi qanday funktsiyalarni bajaradi | \*Elektr signallarini uzatish va qabul qilish |
|  | OSI modelining amaliy satxi qanday funktsiyalarni bajaradi | \*Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub | \*Ethernet, FDDI |
|  | Keltirilgan protokollarning qaysilari taqdimlash satxi protokollariga mansub | \*SNMP, Telnet |
|  | Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu... | \*Avtorizatsiya |
|  | Autentifikatsiya faktorlari nechta | 4 |
|  | Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima | Login |
|  | Ko‘z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar? | Biron nimaga egalik asosida |
|  | barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi? | \*Fizik satx |
|  | Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi | \*2 |
|  | Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? | \*Foydalanishni boshqarish |
|  | Foydalanishni boshqarish –bu... | Subyektni Subyektga ishlash qobilyatini aniqlashdir. |
|  | Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi? | Obyekt |
|  | Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ? | \*Obyekt |
|  | Foydalanishna boshqarishning nechta usuli mavjud? | \*4 |
|  | Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo‘llaniladi | ABAC |
|  | Foydalanishni boshqarishning qaysi modelida Obyekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi | ABAC |
|  | Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi. | ABAC |
|  | Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bog‘liq.. | Tashkilotda Obyektning muhimlik darajasi bilan yoki yuzaga keladigan foyda miqdori bilan bilan xarakterlanadi |
|  | MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi | \*xavfsizlik siyosati ma’muri |
|  | Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi | Yozish |
|  | Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi. | \*Yozish |
|  | Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun Obyektlardan foydalanish ruxsati ko‘rsatiladi? | ABAC |
|  | Rol tushunchasiga ta’rif bering. | \*Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin |
|  | Foydalanishni boshqarishning qaysi usuli - Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. | \*ABAC |
|  | XACML foydalanishni boshqarishni qaysi usulining standarti? | \*ABAC |
|  | Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan? | \*barchasi |
|  | Axborotning kriptografik himoya vositalari necha turda? | 4 |
|  | Dasturiy shifrlash vositalari necha turga bo‘linadi | \*4 |
|  | Diskni shifrlash nima uchun amalga oshiriladi? | \*Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi |
|  | Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi? | 8 |
|  | Kompyuter tarmoqlari bu – | \*Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi |
|  | Tarmoq modeli –bu.. ikki | Matematik modellar to‘plami |
|  | OSI modelida nechta tarmoq satxi bor | \*7 |
|  | OSI modeli 7 satxi bu | \*Ilova |
|  | OSI modeli 1 satxi bu | Ilova |
|  | OSI modeli 2 satxi bu | Ilova |
|  | TCP/IP modelida nechta satx mavjud | \*4 |
|  | Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi? | Lokal |
|  | Tarmoq kartasi bu... | \*Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Switch bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Hab bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Tarmoq repiteri bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi. | \*DNS tizimlari |
|  | ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. | \*TCP |
|  | …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi. | \*UDP |
|  | Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi. | TCP |
|  | Tarmoq taxdidlari necha turga bo‘linadi | 2 |
|  | Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; | \*Razvedka hujumlari |
|  | Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi | Razvedka hujumlari |
|  | Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi; | Razvedka hujumlari |
|  | Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi; | Razvedka hujumlari |
|  | RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart? | \*e soni Eyler funksiyasi - bilan o‘zaro tub |
|  | RSA elektron raqamli imzo algoritmidagi yopiq kalit  d qanday hisoblanadi? Bu yerda p va q tub sonlar,n=pq, - Eyler funksiyasi,e-ochiq kalit | \* |
|  | Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? | \*Imzo qo‘yish va imzoni tekshirishdan |
|  | Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? | \*Imzo muallifining ochiq *kaliti yordamida* |
|  |  |  |

|  |
| --- |
| **Tarmoq modeli-bu...** |
| \*Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar  muvaffaqqiyatli o‘rnatilishini asosidir |
|  | OSI modeli nechta satxga ajraladi? | 2 |
|  | Fizik satxning vazifasi nimadan iborat | \*Qurilma, signal va binar o‘zgartirishlar |
|  | Ilova satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | Kanal satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | Tarmoq satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | TCP/IP modeli nechta satxdan iborat | \*4 |
|  | Quyidagilarninf qaysi biri Kanal satxi protokollari | \*Ethernet, Token Ring, FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri tarmoq satxi protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri transport satxi protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri ilova satxi protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi | \*Kanal, Fizik |
|  | TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi | Kanal, Fizik |
|  | TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi | Kanal, Fizik |
|  | TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos keladi | Kanal, Fizik |
|  | Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang. | \*Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan | \*Tarmoqda har bir kompyuter yoki tugun Markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Tarmoq kartasi nima? | \*Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Repetir nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Hub nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Switch nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Router nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | DNS tizimlari. | \*Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi |
|  | TCP bu- … | \*Transmission Control Protocol |
|  | UDP bu-… | User domain protocol |
|  | IP protokolining necha xil versiyasi mavjud? | 1 |
|  | Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang | \*Ichki, tashqi |
|  | Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi | \*Biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi | \*Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya  usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya  usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi | \*Razvedka hujumlari |
|  | Razvedka hujumiga berilgan ta’rifni aniqlang | \*Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
|  | Kirish hujumiga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axboro ni to‘plashni maqsad qiladi; |
|  | DOS hujumiga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
|  | Zararli hujumga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
|  | Razvetka hujumari necha turga bo’linadi | 1 |
|  | Qaysi hujum jarayoni TCP/IP tarmog‘ida paketlarni tutib  olish, dekodlash, tekshirish va tarjima qilishni o‘z ichiga  oladi | \*Paketlarni snifferlash |
|  | Tarmoqlaro ekranni OSI modeli bo’yicha qanday turlarga bo’lindi? | \*• paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida |
|  | Tarmoqlaro ekranni foydalanilgan texnologiyasi bo’yicha qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida |
|  | Tarmoqlaro ekranni bajarilishiga ko’ra qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida |
|  | Tarmoqlaro ekranni ulanish sxemasi bo’yicha qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahidaishlaydi; ilova proksilari – ilova satxida |
|  | Paket filtrlari tarmoqlararo ekrani vazifasi nima? | \*Tarmoq satxida paketlarni  tahlillashga asoslan; |
|  | Ilova proksilari tarmoqlararo ekrani vazifasi nima? | Tarmoq satxida paketlarni tahlillashga asoslan; |
|  | Ekspert paket filtrlari tarmoqlararo ekrani vazifasi nima? | Tarmoq satxida paketlarni tahlillashga asoslan; |
|  | Quyidagilardan qaysi biri paket filtrlari tarmoqlararo ekrani kamchiligini ifodalaydi. | \*Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma’lumotlarni, zararli dasturlarni va hak. tekshirmaydi. |
|  | Quyidagilardan qaysi biri ekspert paket filtrlari tarmoqlararo ekrani kamchiligini ifodalaydi. | Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma’lumotlarni, zararli  dasturlarni va hak. tekshirmaydi. |
|  | Simsiz tarmoqlarning nechta turi mavjud | 5 |
|  | Bluetooth qanday simsiz tarmoq turiga kiradi. | Global |
|  | Wifi qanday simsiz tarmoq turiga kiradi. | Global |
|  | LTE, CDMA, HSDPA qanday simsiz tarmoq turiga kiradi. | \*Global |
|  | WiMAX qanday simsiz tarmoq turiga kiradi. | Global |
|  | Bluetooth texnologiyasida autentifikatsiya bu… | Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. |
|  | Bluetooth texnologiyasida konfidensiallik bu… | \*Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. |
|  | Bluetooth texnologiyasida avtorizatsiya bu… | Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. |
|  | GSM bu ..- | \*Global System for Mobile Communications |
|  | Simsiz tarmoq Bluetooth ishlash rejimlari nechta? | 2 |
|  | Kompyuterda hodisalar haqidagi ma’lumot qayerda saqlanadi? | \*hodisalar jurnaliga |
|  | Windows operatsion tizimida xatolik hodisasiga berilgan ta’rifni belgilang. | \*Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
|  | Windows operatsion tizimida ogohlantirish hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
|  | Windows operatsion tizimida axborot hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
|  | Windows operatsion tizimida muvaffaqiyatli audit hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
|  | Windows operatsion tizimida muvaffaqiyatsiz audit hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
|  | Ma’lumotlarni zaxira nusxalash bu – … | \*Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi |
|  | Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz | \*Zaxira nusxalash |
|  | Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering | \*Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Ma’lumotlarni g’arazli hatti harakatlar yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Ma’lumotlarni tasodifiy sabablar tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Ma’lumotlarni tabiiy ofatlar tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi? | 7 |
|  | Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. | \*4 |
|  | Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash | \*Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | Zaxira nusxalovchi vositalar tanlashdagi *ishonchlilik* xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | Zaxira nusxalovchi vositalar tanlashdagi tezlik xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | Zaxira nusxalovchi vositalar tanlashdagi foydalanuvchanlik xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | Zaxira nusxalovchi vositalar tanlashdagi qulaylik xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | RAID texnologiyasining transkripsiyasi qanday. | Redundant Array of Independent Disks |
|  | RAID texnologiyasida nechta satx mavjud | 3 |
|  | RAID 0: diskni navbatlanishi bu-.. | \*Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi. Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
|  | RAID 1: diskni navbatlanishi bu-.. | Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi.  Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
|  | RAID 3: diskni navbatlanishi bu-.. | Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi.  Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
|  | RAID 5: diskni navbatlanishi bu-.. | Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi.  Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
|  | RAID 10: diskni navbatlanishi bu-.. | \*Gibrid satx bo‘lib, RAID 1 va RAID 0  satxlaridan iborat va kamida 4 ta diskni talab etadi |
|  | RAID 50: diskni navbatlanishi bu-.. | Gibrid satx bo‘lib, RAID 1 va RAID 0  satxlaridan iborat va kamida 4 ta diskni talab etadi |
|  | Ma’lumotlarni nusxalash usullari necha xil usulda amalga oshiriladi? | \*3 |
|  | Issiq zaxiralash usuliga berilgan ta’rifni belgilang. | \*Ushbu usulda foydalanuvchi tizimni boshqarayotgan  vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.  Mazkur zaxiralash usulini amalga oshirish tizimni  harakatsiz vaqtini kamaytiradi. |
|  | Iliq zaxiralash usuliga berilgan ta’rifni belgilang. | Ushbu usulda foydalanuvchi tizimni boshqarayotgan  vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.  Mazkur zaxiralash usulini amalga oshirish tizimni  harakatsiz vaqtini kamaytiradi. |
|  | Sovuq zaxiralash usuliga berilgan ta’rifni belgilang. | Ushbu usulda foydalanuvchi tizimni boshqarayotgan  vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.  Mazkur zaxiralash usulini amalga oshirish tizimni  harakatsiz vaqtini kamaytiradi. |
|  | Ichki zahiralash qanday amalga oshiriladi | Ichki zahiralashda mahalliy yoki global serverlardan foydalaniladi |
|  | OSI modelining birinchi satxi qanday nomlanadi | \*Fizik satx |
|  | OSI modelining ikkinchi satxi qanday nomlanadi | \*Kanal satxi |
|  | OSI modelining uchinchi satxi qanday nomlanadi | \*Tarmoq satxi |
|  | OSI modelining oltinchi satxi qanday nomlanadi | \*Taqdimlash satxi |
|  | OSI modelining ettinchi satxi qanday nomlanadi | \*Amaliy satx |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi | \*Fizik satx |
|  | Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub | \*TCP,UDP |
|  | OSI modelining fizik satxi qanday funktsiyalarni bajaradi | \*Elektr signallarini uzatish va qabul qilish |
|  | OSI modeliningamaliy satxi qanday funktsiyalarni bajaradi | \*Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | 12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan sonlar soni nechta? | 6 ta |
|  | Yevklid algoritmi qanday natijani beradi? | \*Sonning eng katta umumiy bo’luvchisini toppish |
|  | Qanday sonlar tub sonlar deb yuritiladi? | \*Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi. |
|  | To‘liq zaxiralash | Tiklashning tezligi yuqori. axira nusxalash jarayonining sekin va ma’lumotni saqlash  uchun ko‘p hajm talab etadi |
|  | O‘sib boruvchi zaxiralash | Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi |
|  | Differnsial zaxiralash | Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi |
|  | Ushbu jarayon ma’lumot qanday yo‘qolgani, ma’lumotni qayta tiklash dasturiy vositasi va ma’lumotni tiklash anzilini qayergaligiga bog‘liq bo‘ladi. Qaysi jarayon | Ma’lumotlarni qayta tiklash |
|  | Antivirus dasturlarini ko’rsating? | \*Drweb, Nod32, Kaspersky |
|  | Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi | \*wep, wpa, wpa2 |
|  | Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak? | \*ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | \*bit |
|  | Virtual xususiy tarmoq – bu? | \*VPN |
|  | Xavfli viruslar bu - … | \*kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | \*Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Rezident virus... | \*tezkor xotirada saqlanadi |
|  | DIR viruslari nimani zararlaydi? | \*FAT tarkibini zararlaydi |
|  | .... kompyuter tarmoqlari bo’yicha tarqalib, kompyuterning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi | \*«Chuvalchang» va replikatorli virus |
|  | Mutant virus... | \*shifrlash va deshifrlash algoritmlaridan iborat |
|  | Fire Wall ning vazifasi... | \*tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi |
|  | Kompyuter virusi nima? | \*maxsus yozilgan va zararli dastur |
|  | Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating | \*disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali |
|  | Troyan dasturlari bu... | \*virus dasturlar |
|  | Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? | \*5 |
|  | Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud | \*detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | \*kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya mahnosi... | \*sirli yozuv |
|  | …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi | \*K.Shennon |
|  | Kriptologiya yo’nalishlari nechta? | \*2 |
|  | Kriptografiyaning asosiy maqsadi... | \*maxfiylik, yaxlitlilikni ta`minlash |
|  | Zararli dasturiy vositalarni aniqlash turlari nechta | \*3 |
|  | Signaiurana asoslangan | \*....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh  qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
|  | O‘zgarishni aniqlashga asoslangan | ....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh  qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
|  | Anomaliyaga asoslangan | ....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh  qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
|  | Antiairuslar qanday usulda viruslarni aniqlaydi | Anomaliyaga asoslangan |
|  | Viruslar - | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Rootkitlar- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Backdoorlar - | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vositasifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Troyan otlari- | \*bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Ransomware- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Resurslardan foydalanish usuliga ko’ra viruslar qanday turlarga bo’linadi | \*Virus parazit, Virus cherv |
|  | Zararlagan obyektlar turiga ko’ra | Virus parazit, Virus cherv |
|  | Faollashish prinspiga ko’ra | Virus parazit, Virus cherv |
|  | Dastur kodini tashkil qilish yondashuviga ko‘ra | Virus parazit, Virus cherv |
|  | Shifrlanmagan viruslar | \*o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | Shifrlangan viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | Polimorf viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | Dasturiy viruslar-… | bir vaqtning o‘zida turli xildagi Obyektlarni  zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. |
|  | Ko‘p platformali viruslar | \*bir vaqtning o‘zida turli xildagi Obyektlarni  zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. |
|  | Yuklanuvchi viruslar | bir vaqtning o‘zida turli xildagi Obyektlarni  zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. |
|  | Makroviruslar-... | bir vaqtning o‘zida turli xildagi Obyektlarni  zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. |
|  | Birinchi kompyuter virusi nima deb nomlangan | Cherv |
|  | P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang | \*840 |
|  | 256mod25=? | 5 |
|  | bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi. | \*Tizim |
|  | Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori satxli hujjat yoki hujjatlar to‘plami nima duyidadi | Standart |
|  | RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday? | 65535; |
|  | DES algoritmi akslantirishlari raundlari soni qancha? | \*16; |
|  | DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha? | CHap qism blok 32 bit, o‘ng qism blok 48 bit; |
|  | Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? | SHifrlash va deshifrlash jarayonlarida kalitlardan foydalanish qoidalariga ko‘ra farqlanadi |
|  | 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta? | 19 ta |
|  | 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta? | \*4 ta |
|  | Qaysi formula qoldiqli bo’lish qonunini ifodalaydi |  |
|  | Eyler funsiyasida 𝜙(1) qiymati nimaga teng? | \*0 |
|  | Eyler funksiyasida 60 sonining qiymatini toping. | 59 |
|  | Eyler funksiyasi yordamida 1811 sonining qiymatini toping. | \*1810 |
|  | 97 tub sonmi? | \*Tub |
|  | Quyidagi modulli ifodani qiymatini toping  (148 + 14432) mod 256. | \*244 |
|  | Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220 | 21 |
|  | Quyidagi ifodani qiymatini toping.  -17mod11 | 6 |
|  | 2 soniga 10 modul bo’yicha teskari sonni toping. | 3 |

1. I:
2. S: Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.
3. +: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik
4. -: Axborot va Iqtisodiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xafvsizligi, Dasturiy ta`minot xavfsizligi
5. -: Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xafvsizligi, Ekologik xavfsizlik
6. -: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Dasturiy ta`minot xavfsizligi, Ekologik xavfsizlik
7. I:
8. S: Axborot xavfsizligining asosiy maqsadlaridan biri- bu…
9. +: Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish
10. -:Ob`yektga bevosita ta`sir qilish
11. -: Axborotlarni shifrlash, saqlash, yetkazib berish
12. -: Tarmoqdagi foydalanuvchilarni xavfsizligini ta`minlab berish
13. I:
14. S: Konfidentsiallikga to’g’ri ta`rif keltiring.
15. +: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
16. -:axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati;
17. -:axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati;
18. -:axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati;
19. I:
20. S: Yaxlitlikni buzilishi bu - …
21. +: Soxtalashtirish va o’zgartirish
22. -: Ishonchsizlik va soxtalashtirish
23. -: Soxtalashtirish
24. -: Butunmaslik va yaxlitlanmaganlik
25. I:
26. S:... axborotni himoyalash tizimi deyiladi.
27. +: Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi
28. -: Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo’qotilishidan keladigan zarar va himoyalash mexanizmining narxidan kelib chiqqan holda axborotni himoyalashning zaruriy darajasi
29. -: Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo’qotilishidan keladigan zarar va himoyalash mexanizmining zaruriy darajasi hamda tizimning turini, himoyalash usullar va vositalari
30. -: Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul
31. I:
32. S: Kompyuter virusi nima?
33. +: maxsus yozilgan va zararli dastur
34. -:.exe fayl
35. -: boshqariluvchi dastur
36. -: Kengaytmaga ega bo’lgan fayl
37. I:
38. S: Kriptografiyaning asosiy maqsadi...
39. +: maxfiylik, yaxlitlilikni ta`minlash
40. -:ishonchlilik, butunlilikni ta`minlash
41. -:autentifikatsiya, identifikatsiya
42. -:ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya
43. I:
44. S: SMTP - Simple Mail Transfer protokol nima?
45. +: elektron pochta protokoli
46. -:transport protokoli
47. -:internet protokoli
48. -:Internetda ommaviy tus olgan dastur
49. I:
50. S: SKIP protokoli...
51. +: Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi
52. -:Protokollar boshqaruvi
53. -:E-mail protokoli
54. -:Lokal tarmoq protokollari uchun kriptokalitlarning oddiy boshqaruvi
55. I:
56. S: Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar…
57. +: uzilish, tutib qolish, o’zgartirish, soxtalashtirish
58. -:o’zgartirish, soxtalashtirish
59. -:tutib qolish, o’zgarish, uzilish
60. -:soxtalashtirish, uzilish, o’zgartirish
61. I:
62. S: ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.
63. +: konfidentsiallik
64. -:identifikatsiya
65. -:autentifikatsiya
66. -: maxfiylik
67. I:
68. S: Foydalanish huquqini cheklovchi matritsa modeli bu...
69. +: Bella La-Padulla modeli
70. -:Dening modeli
71. -:Landver modeli
72. -:Huquqlarni cheklovchi model
73. I:
74. S: Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi?
75. +: TCP/IP, X.25 protokollar
76. -:X.25 protokollar
77. -:TCP/IP
78. -:SMTP
79. I:
80. S: Autentifikatsiya nima?
81. +: Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi
82. -: Tizim meyoriy va g’ayritabiiy hollarda rejalashtirilgandek o’zini tutishligi holati
83. -: Istalgan vaqtda dastur majmuasining mumkinligini kafolati
84. -:Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi
85. I:
86. S:Identifikatsiya bu- …
87. +: Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni
88. -:Ishonchliligini tarqalishi mumkin emasligi kafolati
89. -:Axborot boshlang’ich ko’rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o’zgarishlar
90. -:Axborotni butunligini saqlab qolgan holda uni elementlarini o’zgartirishga yo’l qo’ymaslik
91. I:
92. S:O’rin almashtirish shifri bu - …
93. +: Murakkab bo’lmagan kriptografik akslantirish
94. -:Kalit asosida generatsiya qilish
95. -:Ketma-ket ochiq matnni ustiga qo’yish
96. -:Belgilangan biror uzunliklarga bo’lib chiqib shifrlash
97. I:
98. S:Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.
99. +: 2 turga
100. -:3 turga
101. -:4 turga
102. -: 5 turga
103. I:
104. S: Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular …
105. +: hosil qilish, yig’ish, taqsimlash
106. -:ishonchliligi, maxfiyligi, aniqligi
107. -:xavfsizlik, tez ishlashi, to’g’ri taqsimlanishi
108. -:abonentlar soni, xavfsizligi, maxfiyligi
109. I:
110. S: Kriptologiya -
111. +: axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
112. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
113. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
114. -:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
115. I:
116. S: Kriptografiyada alifbo –
117. +: axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
118. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
119. -:xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
120. -:kalit axborotni shifrlovchi kalitlar
121. I:
122. S: Simmetrik kriptotizimlarda ... jumlani davom ettiring
123. +: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi
124. -:bir-biriga matematik usullar bilan bog’langan ochiq va yopiq kalitlardan foydalaniladi
125. -:axborot ochiq kalit yordamida shifrlanadi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi
126. -:kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi
127. I:
128. S: Kriptobardoshlilik deb …
129. +: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
130. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
131. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
132. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
133. I:
134. S: Elektron raqamli imzo deb –
135. +: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
136. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
137. -:axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
138. -:kalit axborotni shifrlovchi kalitlar
139. I:
140. S: Kriptografiya –
141. +: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
142. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
143. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
144. -:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
145. I:
146. S: Kriptografiyada matn –
147. +: alifbo elementlarining tartiblangan to’plami
148. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
149. -:axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
150. -:kalit axborotni shifrlovchi kalitlar
151. I:
152. S: Kriptoanaliz –
153. +: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
154. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
155. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
156. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
157. I:
158. S: Shifrlash –
159. +: akslantirish jarayoni ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi
160. -:kalit asosida shifrmatn ochiq matnga akslantiriladi
161. -:shifrlashga teskari jarayon
162. -:Almashtirish jarayoni bo’lib: ochiq matn deb nomlanadigan matn o’girilgan holatga almashtiriladi
163. I:
164. S: Faol hujum turi deb…
165. +: Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon
166. -:Maxfiy ma`lumotni aloqa tarmog’ida uzatilayotganda eshitish, tahrir qilish, yozib olish harakatlaridan iborat uzatilalayotgan ma`lumotni qabul qiluvchiga o’zgartirishsiz yetkazish jarayoni
167. -:Ma`lumotga o’zgartirish kiritmay uni kuzatish jarayoni
168. -:Sust hujumdan farq qilmaydigan jarayon
169. I:
170. S: Blokli shifrlash-
171. +: shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish
172. -:murakkab bo’lmagan kriptografik akslantirish
173. -:axborot simvollarini boshqa alfavit simvollari bilan almashtirish
174. -:ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi
175. I:
176. S: Simmetrik kriptotizmning uzluksiz tizimida …
177. +: ochiq matnning har bir harfi va simvoli alohida shifrlanadi
178. -:belgilangan biror uzunliklarga teng bo’linib chiqib shifrlanadi
179. -:murakkab bo’lmagan kriptografik akslantirish orqali shifrlanadi
180. -:ketma-ket ochiq matnlarni o’rniga qo’yish orqali shifrlanadi
181. I:
182. S: Kriptotizimga qo’yiladigan umumiy talablardan biri
183. +: shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak
184. -:shifrlash algoritmining tarkibiy elementlarini o’zgartirish imkoniyati bo’lishi lozim
185. -:ketma-ket qo’llaniladigan kalitlar o’rtasida oddiy va oson bog’liqlik bo’lishi kerak
186. -:maxfiylik o’ta yuqori darajada bo’lmoqligi lozim
187. I:
188. S: Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?
189. +: Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi
190. -:Asimmetrik tizimlarda k1=k2 bo’ladi, yahni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi
191. -:Asimmetrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma`lum bo’ladi, ochiq kalitni esa faqat qabul qiluvchi biladi
192. -:Asimmetrik kriptotizimlarda k1≠k2 bo’lib, kalitlar hammaga oshkor etiladi
193. I:
194. S: Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang
195. +: Vijener matritsasi, Sezar usuli
196. -:monoalfavitli almashtirish
197. -:polialfavitli almashtirish
198. -:o’rin almashtirish
199. I:
200. S: Akslantirish tushunchasi deb nimaga aytiladi?
201. +: 1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga
202. -:1-to’plamli elementlariga 2-to’plam elementalrini qarama-qarshiligiga
203. -:har bir elementni o’ziga ko’payimasiga
204. -:agar birinchi va ikinchi to’plam bir qiymatga ega bulmasa
205. I:
206. S: Simmetrik guruh deb nimaga aytiladi?
207. +: O’rin almashtirish va joylashtirish
208. -:O’rin almashtirish va solishtirish
209. -:Joylashtirish va solishtirish
210. -:O’rin almashtirish va transportizatsiyalash
211. I:
212. S: Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?
213. +: simmetrik kriptosistemalar
214. -:assimetrik kriptosistemalar
215. -:ochiq kalitli kriptosistemalar
216. -:autentifikatsiyalash
217. I:
218. S: Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?
219. +: SMTP, POP yoki IMAP
220. -:SKIP, ATM, FDDI
221. -:X.25 va IMAR
222. -:SMTP, TCP/IP
223. I:
224. S: Axborot resursi – bu?
225. +: axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi
226. -:cheklanmagan doiradagi shaxslar uchun mo’ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar
227. -:identifikatsiya qilish imkonini beruvchi rekvizitlari qo’yilgan holda moddiy jismda qayd etilgan axborot
228. -:manbalari va taqdim etilish shaklidan qathi nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to’g’risidagi ma`lumotlar
229. I:
230. S: Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu?
231. +: login parol
232. -:identifikatsiya
233. -:maxfiy maydon
234. -: token
235. I:
236. S: Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu?
237. +: parol
238. -:login
239. -:identifikatsiya
240. -:maxfiy maydon foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
241. I:
242. S: Identifikatsiya jarayoni qanday jarayon?
243. +: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
244. -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
245. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
246. -:foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
247. I:
248. S: Autentifikatsiya jarayoni qanday jarayon?
249. +: obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
250. -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
251. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
252. -:foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
253. I:
254. S: Ro’yxatdan o’tish bu?
255. +: foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
256. -:axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
257. -:ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
258. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
259. I:
260. S: Axborot qanday sifatlarga ega bo’lishi kerak?
261. +: ishonchli, qimmatli va to’liq
262. -:uzluksiz va uzlukli
263. -:ishonchli, qimmatli va uzlukli
264. -:ishonchli, qimmatli va uzluksiz
265. I:
266. S: Axborotning eng kichik o’lchov birligi nima?
267. +: bit
268. -:kilobayt
269. -:bayt
270. -:bitta simvol
271. I:
272. S: Elektron hujjatning rekvizitlari nechta qismdan iborat?
273. +: 4
274. -:5
275. -:6
276. -:7
277. I:
278. S: Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?
279. +: fleshka, CD va DVD disklar
280. -:Qattiq disklar va CDROM
281. -:CD va DVD, DVDROM
282. -:Qattiq disklar va DVDROM
283. I:
284. S: Avtorizatsiya jarayoni qanday jarayon?
285. +: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
286. -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va -berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
287. -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash.
288. -: parollash jarayoni
289. I:
290. S: Kodlash nima?
291. +: Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir
292. -:Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi
293. mumkin bo‘ladi
294. -:Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi
295. mumkin bo‘ladi
296. -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi
297. I:
298. S: Shifrlash nima?
299. +: Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi
300. -:Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir
301. -: Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi
302. -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi
303. I:
304. S: Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi
305. +:Kriptoanaliz
306. -:Kartografiya
307. -:Kriptologiya
308. -:Adamar usuli
309. I:
310. S: Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi
311. +: {d, n} – yopiq, {e, n} – ochiq;
312. -:{d, e} – ochiq, {e, n} – yopiq;
313. -:{e, n} – yopiq, {d, n} – ochiq;
314. -:{e, n} – ochiq, {d, n} – yopiq;
315. I:
316. S: Zamonaviy kriptografiya qanday bo’limlardan iborat?
317. -:Electron raqamli imzo; kalitlarni boshqarish
318. -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;
319. +: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish
320. -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; kalitlarni boshqarish
321. I:
322. S: Shifr nima?
323. +: Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm
324. -:Kalitlarni taqsimlash usuli
325. -:Kalitlarni boshqarish usuli
326. -:Kalitlarni generatsiya qilish usuli
327. I:
328. S: Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?
329. +: Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi
330. -:Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi
331. -:Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin
332. -:Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat deshifrlash mumkin
333. I:
334. S: Oqimli shifrlashning mohiyati nimada?
335. +: Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,
336. -:Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur,
337. -:Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi
338. -:Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,
339. I:
340. S: Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating.
341. +: uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim,
342. -:uzatilayotgan xabarni xavfsizligi kalitni maxfiyligiga emas, balki algoritmni maxfiyligiga bog’liq bo’lishi lozim
343. -:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog’liq bo’lishi lozim
344. -:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga emas, balki shifrlashda foydalaniladigan arifmetik amallar soniga bog’liq bo’lishi lozim
345. I:
346. S: Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?
347. +: shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun
348. -:ERI yaratish va tekshirish, kalitlar almashish uchun
349. -:shifrlash, deshifrlash, kalitlar almashish uchun
350. -: Heshlash uchun
351. I:
352. S: Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi.
353. +: ochiq kalitlar
354. -:yopiq kalitlar
355. -:seans kalitlari
356. -:Barcha tutdagi kalitlar
357. I:
358. S: Kompyuterning tashqi interfeysi deganda nima tushuniladi?
359. +: kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari
360. -:tashqi qurilmani kompyuterga bog’lashda ishlatiladigan ulovchi simlar
361. -:kompyuterning tashqi portlari.
362. -:tashqi qurilma bilan kompyuter o’rtasida axborot almashinish qoidalari to’plami
363. I:
364. S: Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?
365. +: Yulduz
366. -:Xalqa
367. -:To’liqbog’langan
368. -:Umumiy shina
369. I:
370. S: Ethernet kontsentratori qanday vazifani bajaradi
371. +: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi
372. -:kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo’naltirib beradi
373. -:kompyuterdan kelayotgan axborotni xalqa bo’ylab joylashgan keyingi kompyuterga
374. -:tarmoqning ikki segmentini bir biriga ulaydi
375. I:
376. S: OSI modelida nechta satx mavjud
377. +: 7
378. -:4
379. -:5
380. -:3
381. I:
382. S: OSI modelining to’rtinchi satxi qanday nomlanadi
383. +: Transport satxi
384. -:Amaliy satx
385. -:Seanslar satxi
386. -:Taqdimlash satxi
387. I:
388. S: OSI modelining beshinchi satxi qanday nomlanadi
389. +: Seanslar satxi
390. -:Tarmoq satxi
391. -:Fizik satx
392. -:Amaliy satx
393. I:
394. S: OSI modelining birinchi satxi qanday nomlanadi
395. +: Fizik satx
396. -:Seanslar satxi
397. -:Transport satxi
398. -:Taqdimlash satxi
399. I:
400. S: OSI modelining ikkinchi satxi qanday nomlanadi
401. +: Kanal satxi
402. -:Amaliy satxi
403. -:Fizik satx
404. -:Seanslar satxi
405. I:
406. S: OSI modelining uchinchi satxi qanday nomlanadi
407. +: Tarmoq satxi
408. -:Amaliy satx
409. -:Kanal satxi
410. -:Taqdimlash satxi
411. I:
412. S: OSI modelining oltinchi satxi qanday nomlanadi
413. +: Taqdimlash satxi
414. -:Amaliy satx
415. -:Seanslar satxi
416. -:Kanal satxi
417. I:
418. S: OSI modelining yettinchi satxi qanday nomlanadi
419. +: Amaliy satx
420. -:Seanslar satxi
421. -:Transport satxi
422. -:Taqdimlash satxi
423. I:

S: OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi

1. +: fizik, kanal va tarmoq satxlari
2. -:seans va amaliy satxlar
3. -:amaliy va taqdimlash satxlari
4. -:transport va seans satxlari
5. I:
6. S: OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi
7. +: Marshrutizator
8. -:Ko’prik
9. -:Tarmoq adapter
10. -:Kontsentrator
11. I:
12. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
13. +: Fizik satx
14. -:Kanal satxi
15. -:Tarmoq satxi
16. -:Transport satxi
17. I:
18. S: Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi
19. +: Tarmoq satxi
20. -:Kanal satxi
21. -:Amaliy satx
22. -:Transport satxi
23. I:
24. S: Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub
25. +: IP, IPX
26. -:NFS, FTP
27. -:Ethernet, FDDI
28. -:TCP,UDP
29. I:
30. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
31. +: TCP,UDP
32. -:NFS, FTP
33. -:IP, IPX
34. -:Ethernet, FDDI
35. I:
36. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
37. +: Elektr signallarini uzatish va qabul qilish
38. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojaat qilishni boshqarish
39. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
40. -:Klient dasturlari bilan o’zaro muloqotda bo’lish
41. I:
42. S: Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...
43. +: Avtorizatsiya
44. -:Shifrlash
45. -:Identifikatsiya
46. -:Autentifikatsiya
47. I:
48. S: Autentifikatsiya faktorlari nechta
49. +: 3
50. -:4
51. -:5
52. -: 6
53. I:
54. S: Ko‘z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar?
55. +: Biometrik autentifikatsiya
56. -:Biron nimaga egalik asosida
57. -:Biron nimani bilish asosida
58. -:Parolga asoslangan
59. I:
60. S: Barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi?
61. +: Fizik satx
62. -:Tarmoq satxi
63. -:Amaliy satx
64. -:Tadbiqiy sath
65. I:
66. S: Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi
67. +: 2
68. -:4
69. -:3
70. -:5
71. I:
72. S: Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?
73. +: Subyekt
74. -:Obyekt
75. -:Tizim
76. -:Jarayon
77. I:
78. S: MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi
79. +: xavfsizlik siyosati ma’muri
80. -:Foydalaguvchining o‘zi
81. -:Dastur tomonidan
82. -:Boshqarish amaalga oshirilmaydi
83. I:
84. S: Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi
85. +: O‘qish
86. -:Yozish
87. -:O‘zgartirish
88. -:Yashirish
89. I:
90. S: Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.
91. +: Yozish
92. -:O‘qish
93. -:O‘zgartirish
94. -:Yashirish
95. I:
96. S: Rol tushunchasiga ta’rif bering.
97. +: Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin
98. -:Foydalanishni boshqarish
99. -:Muayyan faoliyat turi bilan bog‘liq imkoniyatlar to‘plami sifatida belgilanishi mumkin
100. -:Vakolitlarni taqsimlash
101. I:
102. S: Foydalanishni boshqarishning qaysi usuli - Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.
103. +: ABAC
104. -:MAC
105. -:DAC
106. -:RBAC
107. I:
108. S: Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?
109. +: barchasi
110. -:bimetrik alomatlarning ishga layoqatli shaxsdan ajratib bo‘lmasligi
111. -:biometrik alomatlarni soxtalashtirishning qiyinligi
112. -:biometrik alomatlarni noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasi yuqoriligi
113. I:
114. S: OSI modeli 7 satxi bu
115. +: Ilova
116. -:Seans
117. -:Fizik
118. -:Kanal
119. I:
120. S: OSI modeli 1 satxi bu
121. +: Fizik
122. -:Ilova
123. -:Seans
124. -:Kanal
125. I:
126. S: OSI modeli 2 satxi bu
127. +:Kanal
128. -: Fizik
129. -:Ilova
130. -:Seans
131. I:
132. S: TCP/IP modelida nechta satx mavjud
133. +: 4
134. -:3
135. -:2
136. -:8
137. I:
138. S: Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi?
139. +: Shaxsiy tarmoq
140. -:Lokal
141. -:Mintaqaviy
142. -:CAMPUS
143. I:
144. S: Tarmoq kartasi bu...
145. +: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
146. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.
147. -:ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
148. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
149. I:
150. S: Server xotirasidagi joyni bepul yoki pulli ijagara berish xizmati qanday ataladi?

1. +: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
2. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
3. -:Signalni tiklash yoki qaytarish uchun foydalaniladi.
4. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
5. I:
6. S: Hab bu...
7. +: ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
8. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
9. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.
10. -:qabul qilingan signalni barchachiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
11. I:
12. S: Tarmoq repiteri bu...
13. +: Signalni tiklash yoki qaytarish uchun foydalaniladi.
14. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
15. -:ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
16. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
17. I:
18. S: Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi.
19. +: DNS tizimlari
20. -:TCP/IP
21. -:Ethernet
22. -:Token ring
23. I:
24. S: ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.
25. +: TCP
26. -:IP
27. -:HTTP
28. -:FTP
29. I:
30. S: …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.
31. +: UDP
32. -:HTTP
33. -:TCP
34. -:FTP
35. I:
36. S: Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi.
37. +: IP
38. -:TCP
39. -:HTTP
40. -:FTP
41. I:
42. S: Tarmoq taxdidlari necha turga bo‘linadi
43. +: 4
44. -:2
45. -:3
46. -:5
47. I:
48. S: Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;
49. +: Razvedka hujumlari
50. -:Kirish hujumlari
51. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
52. -:Zararli hujumlar
53. I:
54. S: Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi
55. +: Kirish hujumlari
56. -:Razvedka hujumlari
57. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
58. -:Zararli hujumlar
59. I:
60. S: Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;
61. +: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
62. -:Razvedka hujumlari
63. -:Kirish hujumlari
64. -:Zararli hujumlar
65. I:
66. S: Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;
67. +: Zararli hujumlar
68. -:Razvedka hujumlari
69. -:Kirish hujumlari
70. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
71. I:
72. S: RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart?
73. +: e soni Eyler funksiyasi - bilan o‘zaro tub
74. -:e ning qiymati [1,n] kesmaga tegishli ixtiyoriy son
75. -:e soni ixtiyoriy tub son
76. -:e soni ixtiyoriy butun musbat son
77. I:
78. S: RSA elektron raqamli imzo algoritmidagi yopiq kalit d qanday hisoblanadi? Bu yerda p va q tub sonlar,n=pq, - Eyler funksiyasi,e-ochiq kalit
79. +:
80. -:
81. -:
82. -:
83. I:
84. S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?
85. +: Imzo qo‘yish va imzoni tekshirishdan
86. -:Faqat imzo qo‘yishdan
87. -:Faqat imzoni tekshirishdan

1. -:Barcha javoblar to‘g‘ri
2. I:
3. S: Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi?
4. +: Imzo muallifining ochiq kaliti yordamida
5. -:Ma’lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida
6. -:Ma’lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida
7. -:Imzo muallifining maxfiy kaliti yordamida
8. I:
9. S: Tarmoq modeli-bu...
10. +: Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir
11. -:Global tarmoq qurish usullari
12. -:Lokal tarmoq qurish usullari
13. -:To‘g‘ri javob yo‘q.
14. I:
15. S: OSI modeli nechta satxga ajraladi?
16. +: 7
17. -:2
18. -:4
19. -:3
20. I:
21. S: TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi
22. +: Kanal, Fizik
23. -:Tarmoq
24. -:Tramsport
25. -:Ilova, taqdimot, seans.
26. I:
27. S: TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi
28. +: Tarmoq
29. -:Kanal, Fizik
30. -:Tramsport
31. -:Ilova, taqdimot, seans.
32. I:
33. S: TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi
34. +: Tramsport
35. -:Kanal, Fizik
36. -:Tarmoq
37. -:Ilova, taqdimot, seans.
38. I:
39. S: TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos keladi
40. +: Ilova, taqdimot, seans
41. -:Kanal, Fizik
42. -:Tarmoq
43. -:Tramsport
44. I:
45. S: Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.
46. +: Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
47. -:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
48. -:Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi
49. -:Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi
50. I:
51. S: Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.
52. +: Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
53. -:Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
54. -:Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi
55. -:Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi.
56. I:
57. S: Repetir nima?
58. +: Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
59. -:Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
60. -: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
61. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
62. I:
63. S: Hub nima?
64. +: Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
65. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi, Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
66. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
67. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
68. I:
69. S: Router nima?
70. +: Qabul qilingan ma’lumotlarni tarmoq satxiga tegishli manzillarga ko‘ra (IP manzil) uzatadi.
71. -:Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
72. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
73. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
74. I:
75. S: Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi
76. +: Razvedka hujumlari
77. -:Kirish hujumlari
78. -:DOS hujumi
79. -:Zararli hujumlar
80. I:
81. S: Razvedka hujumiga berilgan ta’rifni aniqlang
82. +: Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;
83. -:hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi hujumchi -:mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;
84. -:zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;
85. I:
86. S: OSI modelining birinchi satxi qanday nomlanadi
87. +: Fizik satx
88. -:Seanslar satxi
89. -:Transport satxi
90. -:Taqdimlash satxi
91. I:
92. S: OSI modelining ikkinchi satxi qanday nomlanadi
93. +: Kanal satxi
94. -:Amaliy satxi
95. -:Fizik satx
96. -:Seanslar satxi
97. I:
98. S: OSI modelining uchinchi satxi qanday nomlanadi
99. +: Tarmoq satxi
100. -:Amaliy satx
101. -:Kanal satxi
102. -:Taqdimlash satxi
103. I:
104. S: OSI modelining oltinchi satxi qanday nomlanadi
105. +: Taqdimlash satxi
106. -:Amaliy satx
107. -:Seanslar satxi
108. -:Kanal satxi
109. I:
110. S: OSI modelining ettinchi satxi qanday nomlanadi
111. +: Amaliy satx
112. -:Seanslar satxi
113. -:Transport satxi
114. -:Taqdimlash satxi
115. I:
116. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
117. +: Fizik satx
118. -:Kanal satxi
119. -:Tarmoq satxi
120. -:Transport satxi
121. I:
122. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
123. +: TCP,UDP
124. -:NFS, FTP
125. -:IP, IPX
126. -:Ethernet, FDDI
127. I:
128. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
129. +: Elektr signallarini uzatish va qabul qilish
130. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
131. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
132. -:Klient dasturlari bilan o’zaro muloqotda bo’lish
133. I:
134. S: OSI modelining amaliy satxi qanday funksiyalarni bajaradi
135. +: Klient dasturlari bilan o’zaro muloqotda bo’lish
136. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
137. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
138. -:Elektr signallariniuzatish va qabul qilish
139. I:
140. S: Yevklid algoritmi qanday natijani beradi?
141. +: Sonning eng katta umumiy bo’luvchisini toppish
142. -:Sonning turli bo’luvchilarini toppish
143. -:Sonning eng kichik umumiy karralisini toppish
144. -:Sonning eng katta umumiy bo’linuvchisini topish
145. I:
146. S: Qanday sonlar tub sonlar deb yuritiladi?
147. +: Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi.
148. -:O’zidan boshqa bo’luvchilari mavjud bo’lgan sonlar tub sonlar deyiladi.
149. -:Agar sonning 1 dan boshqa bo’luvchilari bo’lsa.
150. -:Faqatgina 1 ga o’ziga bo’linmaydigan sonlar tub sonlar deyiladi.
151. I:
152. S: OSI modelining birinchi satxi qanday nomlanadi
153. +: Fizik satx
154. -:Seanslar satxi
155. -:Transport satxi
156. -:Taqdimlash satxi
157. I:
158. S: OSI modelining ikkinchi satxi qanday nomlanadi
159. +: Kanal satxi
160. -:Amaliy satxi
161. -:Fizik satx
162. -:Seanslar satxi
163. I:
164. S: OSI modelining uchinchi satxi qanday nomlanadi
165. +: Tarmoq satxi
166. -:Amaliy satx
167. -:Kanal satxi
168. -:Taqdimlash satxi
169. I:
170. S: OSI modelining oltinchi satxi qanday nomlanadi
171. +: Taqdimlash satxi
172. -:Amaliy satx
173. -:Seanslar satxi
174. -:Kanal satxi
175. I:
176. S: OSI modelining ettinchi satxi qanday nomlanadi
177. +: Amaliy satx
178. -:Seanslar satxi
179. -:Transport satxi
180. -:Taqdimlash satxi
181. I:
182. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
183. +: Fizik satx
184. -:Kanal satxi
185. -:Tarmoq satxi
186. -:Transport satxi
187. I:
188. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
189. +: TCP,UDP
190. -:NFS, FTP
191. -:IP, IPX
192. -:Ethernet, FDDI
193. I:
194. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
195. +: Elektr signallarini uzatish va qabul qilish
196. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
197. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
198. -:Klient dasturlari bilan o’zaro muloqotda bo’lish
199. I:
200. S: OSI modeliningamaliy satxi qanday funktsiyalarni bajaradi
201. +: Klient dasturlari bilan o’zaro muloqotda bo’lish
202. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
203. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
204. -:Elektr signallariniuzatish va qabul qilish
205. I:
206. S: Yevklid algoritmi qanday natijani beradi?
207. +: Sonning eng katta umumiy bo’luvchisini toppish
208. -:Sonning turli bo’luvchilarini toppish
209. -:Sonning eng kichik umumiy karralisini toppish
210. -:Sonning eng katta umumiy bo’linuvchisini topish
211. I:
212. S: Qanday sonlar tub sonlar deb yuritiladi?
213. +: Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi.
214. -:O’zidan boshqa bo’luvchilari mavjud bo’lgan sonlar tub sonlar deyiladi.
215. -:Agar sonning 1 dan boshqa bo’luvchilari bo’lsa.
216. -:Faqatgina 1 ga o’ziga bo’linmaydigan sonlar tub sonlar deyiladi.
217. I:
218. S: Antivirus dasturlarini ko’rsating?
219. +: Drweb, Nod32, Kaspersky
220. -:arj, rar, pkzip, pkunzip
221. -:winrar, winzip, winarj
222. -:pak, lha
223. I:
224. S: Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi
225. +: wep, wpa, wpa2
226. -:web, wpa, wpa2
227. -:wpa, wpa2
228. -:wpa, wpa2, wap
229. I:
230. S: Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak?
231. +: ishonchli, qimmatli va to’liq
232. -:uzluksiz va uzlukli
233. -:ishonchli, qimmatli va uzlukli
234. -:ishonchli, qimmatli va uzluksiz
235. I:
236. S: Axborotning eng kichik o’lchov birligi nima?
237. +: bit
238. -:kilobayt
239. -:bayt
240. -:bitta simvol
241. I:
242. S: Virtual xususiy tarmoq – bu?
243. +: VPN
244. -:APN
245. -:ATM
246. -:Ad-hoc
247. I:
248. S: Xavfli viruslar bu - …
249. +: kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar
250. -:tizimda mavjudligi turli taassurot (ovoz, video) bilan bog’liq viruslar, bo’sh xotirani kamaytirsada, dastur va ma`lumotlarga ziyon yetkazmaydi
251. -:o’z-o’zidan tarqalish mexanizmi amalga oshiriluvchi viruslar
252. -:dastur va ma`lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o’chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar
253. I:
254. S: Mantiqiy bomba – bu …
255. +: Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari
256. -:Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari
257. -:Viruslar kodiga boshqarishni uzatish
258. -:Qidirishning passiv mexanizmlarini amalga oshiruvchi, yahni dasturiy fayllarga tuzoq qo’yuvchi viruslar
259. I:
260. S: Rezident virus...
261. +: tezkor xotirada saqlanadi
262. -:to’liqligicha bajarilayotgan faylda joylashadi
263. -:ixtiyoriy sektorlarda joylashgan bo’ladi
264. -:alohida joyda joylashadi
265. I:
266. S: DIR viruslari nimani zararlaydi?
267. +: FAT tarkibini zararlaydi
268. -:com, exe kabi turli fayllarni zararlaydi
269. -:yuklovchi dasturlarni zararlaydi
270. -:Operatsion tizimdagi sonfig.sys faylni zararlaydi
271. I:
272. S:.... kompyuter tarmoqlari bo’yicha tarqalib, komlg’yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi
273. +: «Chuvalchang» va replikatorli virus
274. -:Kvazivirus va troyan virus
275. -:Troyan dasturi
276. -:Mantiqiy bomba
277. I:
278. S: Fire Wall ning vazifasi...
279. +: tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi
280. -:kompyuterlar tizimi xavfsizligini ta`minlaydi
281. -:Ikkita kompyuter o’rtasida aloqa o’rnatish jarayonida Internet tarmog’i orasida xavfsizlikni ta`minlaydi
282. -:uy tarmog’i orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi
283. I:
284. S: Kompyuter virusi nima?
285. +: maxsus yozilgan va zararli dastur
286. -:.exe fayl
287. -:boshqariluvchi dastur
288. -:Kengaytmaga ega bo’lgan fayl
289. I:
290. S: Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating
291. +: disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali
292. -: faqat maxsus tashuvchi qurilma orqali
293. -: faqat kompyuter tarmoqlari orqali
294. -:zararlanish yo’llari juda ko’p
295. I:
296. S: Troyan dasturlari bu...
297. +: virus dasturlar
298. -:antivirus dasturlar
299. -:o’yin dasturlari
300. -:yangilovchi dasturlar
301. I:
302. S: Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi?
303. +: 5
304. -:4
305. -:2
306. -:3
307. I:
308. S: Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud
309. +: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar
310. -:detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar
311. -:vaktsinalar, privivkalar, revizorlar, tekshiruvchilar
312. -:privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar
313. I:
314. S: Stenografiya mahnosi...
315. +: sirli yozuv
316. -:sirli xat
317. -:maxfiy axborot
318. -:maxfiy belgi
319. I:
320. S: …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi
321. +: K.Shennon
322. -:Sezar
323. -:U.Xill
324. -:Fon Neyman
325. I:
326. S: Kriptologiya yo’nalishlari nechta?
327. +: 2
328. -:3
329. -:4
330. -:5
331. I:
332. S: Kriptografiyaning asosiy maqsadi...
333. +: maxfiylik, yaxlitlilikni ta`minlash
334. -:ishonchlilik, butunlilikni ta`minlash
335. -:autentifikatsiya, identifikatsiya
336. -:ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya
337. I:
338. S: DES algoritmi akslantirishlari raundlari soni qancha?
339. +: 16;
340. -:14;
341. -:12;
342. -:32;
343. I:
344. S: DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha?
345. +: CHap qism blok 32 bit, o‘ng qism blok 32 bit;
346. -:CHap qism blok 32 bit, o‘ng qism blok 48 bit;
347. -:CHap qism blok 64 bit, o‘ng qism blok 64 bit;
348. -:CHap qism blok 16 bit, o‘ng qism blok 16 bit;
349. I:
350. S: 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta?
351. +: 18 ta;
352. -:19 ta
353. -:11 ta
354. -:9 ta
355. I:
356. S: 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta?
357. +: 3 ta
358. -:7 ta
359. -:8 ta;
360. -:9 ta
361. I:
362. S: Qaysi formula qoldiqli bo’lish qonunini ifodalaydi
363. +: a = *bq + r,* ,
364. -:
365. -:M=r1^k2;
366. -:M=
367. I:
368. S: Eyler funksiyasida p=11 va q=13 sonining qiymatini toping.
369. +: 16
370. -:59
371. -:30
372. -:21
373. I:
374. S: Eyler funksiyasi yordamida 1811 sonining qiymatini toping.
375. +: 1810
376. -:2111
377. -:16
378. -:524
379. I:
380. S: 97 tub sonmi?
381. +: Tub
382. -:murakkab
383. -:Natural
384. -:To’g’ri javob yo’q
385. I:
386. S: Quyidagi modulli ifodani qiymatini toping
387. (148 + 14432) mod 256.
388. +: 244
389. -:200
390. -:156
391. -:154
392. I:
393. S: Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220
394. +: 44
395. -:21
396. -:42
397. -:20
398. I:
399. S: Quyidagi ifodani qiymatini toping. -16mod11
400. +: 6
401. -:5
402. -:7
403. -:11
404. I:
405. S: 2 soniga 10 modul bo’yicha teskari sonni toping.
406. +: Ø
407. -:3
408. -:10
409. -:25
410. I:
411. S: 2 soniga 10 modul bo’yicha teskari sonni toping.
412. +: Ø
413. -:3
414. -:10
415. -:25
416. I:
417. S: DES da dastlabki kalit uzunligi necha bitga teng?
418. +:56 bit
419. -:128 bit
420. -:64 bit
421. -:32 bit
422. I:
423. S: DES da bloklar har birining uzunligi necha bitga teng?
424. +:32 bit
425. -:56 bit
426. -:48 bit
427. -:64 bit
428. I:
429. S: DES da raundlar soni nechta?
430. +:16
431. -:32
432. -:8
433. -:48
434. I:
435. S: Shifrlash kaliti noma’lum bo’lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi
436. +:kriptobardoshlik
437. -:Shifr matn uzunligi
438. -:Shifrlash algoritmi
439. -:Texnika va texnologiyalar
440. I:
441. S: Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo’linadi
442. +:blokli va oqimli
443. -:DES va oqimli
444. -:Feystel va Verman
445. -:SP− tarmoq va IP
446. I:
447. S: DES shifrlash algoritmida shifrlanadigan malumotlar bloki necha bit?
448. +:64
449. -:32
450. -:48
451. -:56
452. I:
453. S: XOR amali qanday amal?
454. +:2 modul bo`yicha qo`shish
455. -:264 modul bo`yicha qo`shish
456. -:232 modul bo`yicha qo`shish
457. -:248 modul bo`yicha qo`shish
458. I:
459. S: 4+31 mod 32 ?
460. +:3
461. -:4
462. -:31
463. -:32
464. I:
465. S: 21+20mod32?
466. +:9
467. -:12
468. -:16
469. -:41
470. I:
471. S: 12+22 mod 32 ?
472. +:2
473. -:12
474. -:22
475. -:32
476. I:
477. S: AES algoritmi bloki uzunligi … bitdan kam bo’lmasligi kerak.
478. +:128
479. -:512
480. -:256
481. -:192
482. I:
483. S: Xesh-:funktsiyani natijasi …
484. +:fiksirlangan uzunlikdagi xabar
485. -:Kiruvchi xabar uzunligidagi xabar
486. -:Kiruvchi xabar uzunligidan uzun xabar
487. -:fiksirlanmagan uzunlikdagi xabar
488. I:
489. S: 2+5 mod32 ?
490. +:7
491. -:32
492. -:2
493. -:5
494. I:
495. S: 97 tub sonmi?
496. +:Tub
497. -:murakkab
498. -:Natural
499. -:To’g’ri javob yo’q
500. I:
501. S: Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing.
502. +:23
503. -:20
504. -:21
505. -:19
506. I:
507. S: Quyidagi ifodani qiymatini toping. -17mod11
508. +:5
509. -:6
510. -:7
511. -:11
512. I:
513. S: Diskni shifrlash nima uchun amalga oshiriladi?
514. +: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
515. -:Xabarni yashirish uchun amalga oshiriladi
516. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi
517. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi
518. I:
519. S: Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?
520. +: 4
521. -:8
522. -:7
523. -:5
524. I:
525. S: OSI modelida nechta tarmoq satxi bor
526. +: 7
527. -:6
528. -:5
529. -:4
530. I:
531. S: Diskni shifrlash nima uchun amalga oshiriladi?
532. +: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
533. -:Xabarni yashirish uchun amalga oshiriladi
534. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi
535. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi
536. I:
537. S: Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?
538. +: 4
539. -:8
540. -:7
541. -:5
542. I:
543. S: OSI modelida nechta tarmoq satxi bor
544. +: 7
545. -:6
546. -:5
547. -:4
548. I:
549. S: “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonun moddadan iborat
550. +:16
551. -:18
552. -:11
553. -:14
554. I:
555. S: Kompyuter etikasi instituti notijoriy tashkilot tomonidan texnologiyani axloqiy nuqta nazardan targ‘ib qilish bo‘yicha nechta etika qoidalari keltirilgan
556. +:10
557. -:18
558. -:11
559. -:14
560. I:
561. S: Kiberjinoyatchilik bu –. . .
562. +: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.
563. -: Kompyuter o‘yinlari
564. -: Faqat banklardan pul o‘g‘irlanishi
565. -: autentifikatsiya jarayonini buzish
566. I:
567. S: Fishing nima?
568. +: Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.
569. -: Ma’lumotlar bazalarini xatoligi
570. -: Mualliflik huquqini buzilishi
571. -: Lug‘at orqali xujum qilish.
572. I:
573. S: Bag nima?
574. +: Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo
575. -: Mualliflik huquqini buzilishi
576. -: Dasturlardagi ortiqcha reklamalar
577. -: Autentifikatsiya jarayonini buzish
578. I:
579. S: Nuqson nima?
580. +: Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi nuqsondir
581. -: Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo
582. -: Dasturlardagi ortiqcha reklamalar
583. -: Autentifikatsiya jarayonini buzish
584. I:
585. S: Quyidagilardan qaysi birida xavfsiz dasturlash tillari keltirilgan.
586. +: C#, Scala, Java
587. -: C, C#, java
588. -: C++, Scala, Java
589. -: Misra-C, Java, c++
590. I:
591. S: Quyidagilardan qaysi biri dasturiy maxsulotlarga qo‘yiladigan xavfsizlik talablari hisoblanidi.
592. +: Vazifaviy, novazifaviy, qolgan talablar
593. -: Qolgan talablar, anaviy taablar, etika talablari
594. -: Vazifaviy, novazifaviy, etika talablari.
595. -: Vazifaviy, etika talablari, foydalanuvchanlik talablari.
596. I:
597. S: Dasturiy ta’minotda kirish va chiqishga aloqador bo‘lgan talablar qanday talablar sirasiga kiradi?
598. +:Vazifaviy
599. -: Novazifaviy
600. -: Etika talablari
601. -: Qolgan talablar
602. I:
603. S: Dasturda tizim amalga oshirishi kerak bo‘lgan vazifalar bu..
604. +:Vazifaviy
605. -: Novazifaviy
606. -: Etika talablari
607. -: Qolgan talablar
608. I:
609. S: Risklarni boshqarishda risklarni aniqlash jarayoni bu-..
610. +: Tashkilot xavfsizligiga ta’sir qiluvchi tashqi va ichki risklarning manbasi, sababi, oqibati va haklarni aniqlash.
611. -: Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta’siri va ehtimolini o‘lchashni ta’minlaydi.
612. -: Risklarni davolash bu – aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni.
613. -: Risk monitoringi yangi risklarni paydo bo‘lish imkoniyatini aniqlash.
614. I:
615. S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.
616. +:"Sovuq saxiralash"
617. -:"Issiq zaxiralash"
618. -:"Iliq saxiralash"
619. -:"To'liq zaxiralash"
620. I:
621. S: Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishi bilan bog'liq bo'lsa bu nima deb yuritiladi?
622. +:Jinoyat sifatida baholanadi
623. -:Rag’bat hisoblanadi
624. -:Buzgunchilik hisoblanadi
625. -:Guruhlar kurashi hisoblanadi
626. I:
627. S: Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun qanday kalit ishlatiladi?
628. +:Ikkita kalit
629. -:Bitta kalit
630. -:Elektron raqamli imzo
631. -:Foydalanuvchi identifikatori
632. I:
633. S:Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?
634. +:Axborot xavfsizligi buzulgan taqdirda ko’rilishi mumkin bo’lgan zarar miqdori bilan
635. -:Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhumligi bilan
636. -:Axborotni noqonuniy foydalanishlardan o’zgartirishlardan va yo’q qilishlardan himoyalanganligi bilan
637. -:Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bilan}
638. I:
639. S:Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?
640. +:Strukturalarni ruxsatsiz modifikatsiyalash
641. -:Tabiy ofat va avariya
642. -:Texnik vositalarning buzilishi va ishlamasligi
643. -:Foydalanuvchilar va xizmat ko‘rsatuvchi hodimlarning hatoliklari}
644. I:
645. S:Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?
646. +:Texnik vositalarning buzilishi va ishlamasligi
647. -:Axborotdan ruhsatsiz foydalanish
648. -:Zararkunanda dasturlar
649. -:An’anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili}
650. I:
651. S:Axborot xavfsizligini ta'minlovchi choralarni ko’rsating?
652. +:1-huquqiy, 2-tashkiliy-ma'muriy, 3-injener-texnik
653. -:1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy
654. -:1-dasturiy, 2-tashkiliy-ma'muriy, 3-huquqiy
655. -:1-aparat, 2-texnikaviy, 3-huquqiy}
656. I:
657. S:Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o’z ichiga oladi
658. +:Xalqaro va milliy huquqiy me’yorlarni
659. -:Tashkiliy va xalqaro me’yorlarni
660. -:Ananaviy va korporativ me’yorlarni
661. -:Davlat va nodavlat tashkilotlarime’yorlarni}
662. I:
663. S:Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?
664. +: Ma’lumotlar butunligi
665. -:Axborotning konfedensialligi
666. -:Foydalanuvchanligi
667. -:Ixchamligi}

1. I:
2. S:Axborotning buzilishi yoki yo‘qotilishi xavfiga olib keluvchi himoyalanuvchi ob’ektga qarshi qilingan xarakatlar qanday nomlanadi?
3. +:Tahdid
4. -:Zaiflik
5. -:Hujum
6. -:Butunlik}
7. I:
8. S:Biometrik autentifikatsiyalashning avfzalliklari-bu:
9. +:Biometrik alomatlarning noyobligi
10. -:Bir marta ishlatilishi
11. -:Biometrik alomatlarni o’zgartirish imkoniyati
12. -:Autentifikatsiyalash jarayonining soddaligi
13. I:
14. S: Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari-bu:
15. +:Foydalanuvchanligi
16. -:Ma’lumotlar butunligi
17. -:Axborotning konfedensialligi
18. -:Ixchamligi
19. I:
20. S:Global simsiz tarmoqning ta`sir doirasi qanday?
21. +:Butun dunyo bo’yicha
22. -:Binolar va korpuslar
23. -:O’rtacha kattalikdagishahar
24. -:Foydalanuvchi yaqinidagi tarmoq
25. I:
26. S: Foydalanuvchini identifikatsiyalashda qanday ma’lumotdan foydalaniladi?
27. +:Identifikatori
28. -:Telefon raqami
29. -:Parol
30. -:Avtorizatsiyasi
31. I:
32. S: Foydalanuvchining tarmoqdagi harakatlarini va resurslardan foydalanishga urinishini qayd etish-bu:
33. +:Ma`murlash
34. -:Autentifikatsiya
35. -:Identifikatsiya
36. -:Sertifikatsiyalash
37. I:
38. S: Kompyuter tizimini ruxsatsiz foydalanishdan himoyalashni, muhim kompyuter tizimlarni rezervlash, o‘g‘irlash va diversiyadan himoyalanishni ta’minlash rezerv elektr manbai, xavfsizlikning maxsus dasturiy va apparat vositalarini ishlab chiqish va amalga oshirish qaysi choralarga kiradi?
39. +:Injener-texnik
40. -:Molyaviy
41. -:Tashkiliy-ma’muriy
42. -:Huquqiy
43. I:
44. S: Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi-bu:
45. +:Autentifikatsiya
46. -:Identifikatsiya
47. -:Ma`murlash (accaunting)
48. -:Avtorizatsiya
49. I:
50. S: O‘zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi–bu:
51. +:Tarmoq viruslari
52. -:Pochta viruslari
53. -:Fayl viruslari
54. -:Protokol viruslari
55. I:
56. S: Qanday viruslar xavfli hisoblanadi?
57. +:kompyuter ishlashida jiddiy nuqsonlarga olib keluvchi
58. -:Jiddiy nuqsonlarga olib kelmaydigan ammo foydalanuvchini chalg'itadigan.
59. -:Katta viruslar va odatda zararli dasturlar
60. -:Passiv viruslar
61. I:
62. S: Rezident bo’lmagan viruslar qachon xotirani zararlaydi?
63. +:Faqat faollashgan vaqtida
64. -:Faqat o’chirilganda
65. -:Kompyuter yoqilganda
66. -:Tarmoq orqali ma’lumot almashishda
67. I:
68. S: Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan iborat?
69. +:Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud
70. -:Tarmoq chetki nuqtalari orasidagi xududning kengligi asosida qurilmalarholati
71. -:Himoya vositalarining chegaralanganligi
72. -:Himoyani amalga oshirish imkoniyati yo‘qligi va ma'lum protokollarning ishlatilishi
73. I:
74. S: Simmetrik shifrlashning noqulayligi – bu:
75. +:Maxfiy kalitlar bilan ayirboshlash zaruriyatidir
76. -:Kalitlar maxfiyligi
77. -:Kalitlar uzunligi
78. -:SHifrlashga ko‘p vaqt sarflanishi va ko'p yuklanishi
79. I:
80. S: Simsiz tarmoqlarni kategoriyalarini to’g’ri ko’rsating?
81. +:Simsiz shaxsiy tarmoq (PAN), simsiz lokal tarmoq (LAN), simsiz regional tarmoq (MAN) va Simsiz global tarmoq (WAN)
82. -:Simsiz internet tarmoq (IAN )va Simsiz telefon tarmoq (WLAN), Simsiz shaxsiy tarmoq (PAN) va Simsiz global tarmoq (WIMAX)
83. -:Simsiz internet tarmoq (IAN) va uy simsiz tarmog’i
84. -:Simsiz chegaralanmagan tarmoq (LAN), simsiz kirish nuqtalari

1. I:
2. S: Sub`ektga ma`lum vakolat va resurslarni berish muolajasi-bu:
3. +:Avtorizatsiya
4. -:Haqiqiylikni tasdiqlash
5. -:Autentifikatsiya
6. -:Identifikasiya

I:

1. S: Tarmoq operatsion tizimining to'g'ri konfiguratsiyasini madadlash masalasini odatda kim hal etadi?
2. +:Tizim ma'muri
3. -:Tizim foydalanuvchisi
4. -:Korxona raxbari
5. -:Operator
6. I:
7. S: Tarmoqlararo ekran texnologiyasi-bu:
8. +:Ichki va tashqi tarmoq o’rtasida filtr va himoya vazifasini bajaradi
9. -:Ichki va tashqi tarmoq o’rtasida axborotni o’zgartirish vazifasini bajaradi
10. -:Qonuniy foydalanuvchilarni himoyalash
11. -:Ishonchsiz tarmoqdan kirishni boshqarish}
12. I:
13. S: Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko’rsating?
14. +:DDoS (Distributed Denial of Service) hujum
15. -:Tarmoq hujumlari
16. -:Dastur hujumlari asosidagi (Denial of Service) hujum
17. -:Virus hujumlari}
18. I:
19. S: Uyishtirilmagan tahdid, ya’ni tizim yoki dasturdagi qurilmaning jismoniy xatoligi – bu…
20. +:Tasodifiy tahdid
21. -:Uyishtirilgan tahdid
22. -:Faol tahdid
23. -:Passiv tahdid
24. I:
25. S: Axborot xavfsizligi qanday asosiy xarakteristikalarga ega?
26. +:Butunlik, konfidentsiallik, foydalana olishlik
27. -:Butunlik, himoya, ishonchlilikni urganib chiqishlilik
28. -:Konfidentsiallik, foydalana olishlik
29. -:Himoyalanganlik, ishonchlilik, butunlik
30. }
31. I:
32. S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.
33. +:"Sovuq saxiralash"
34. -:"Issiq zaxiralash"
35. -:"Iliq saxiralash"
36. -:"To'liq zaxiralash"
37. I:
38. S: Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?
39. +:"Issiq zaxiralash"
40. -:"Sovuq saxiralash"
41. -:"Iliq saxiralash"
42. -:"To'liq zaxiralash"
43. I:
44. S: Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang
45. +:HandyBakcup
46. -:Recuva, R.saver
47. -:Cryptool
48. -:Eset32
49. I:
50. S: O'chirilgan, formatlangan ma'lumotlarni tikovchi dasturni belgilang.
51. +:Recuva, R.saver
52. -:HandyBakcup
53. -:Cryptool
54. -:Eset32
55. I:
56. S: Virtuallashtirishga qaratilgan dasturiy vositalarni belgilang.
57. +:VMware, VirtualBox
58. -:HandyBakcup
59. -:Eset32
60. -:Cryptool
61. I:
62. S: Cloud Computing texnologiyasi nechta katta turga ajratiladi?
63. +:3 turga
64. -:2 turga
65. -:4 turga
66. -:5 turga
67. I:
68. S: O'rnatilgan tizimlar-bu…
69. +:Bu ko'pincha real vaqt hisoblash cheklovlariga ega bo'lgan kattaroq mexanik yoki elektr tizimidagi maxsus funksiyaga ega, boshqaruvchidir
70. -:Korxona ichki tarmog’iga ulangan korporativ tarmog’idan bo'ladigan hujumlardan himoyalash
71. -:Korxona ichki tarmog’ini Internet global tarmog’idan ajratib qo’yish
72. -:Bu ko'pincha global tizimda hisoblash cheklovlariga ega bo'lgan mexanik yoki elektr tizimidagi maxsus funksiyaga ega qurilmadir
73. I:
74. S: Axborotdan oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan?
75. +:AQSH sog'liqni saqlash va insonlarga xizmat ko'rsatish vazirligi
76. -:AQSH Mudofaa vazirligi
77. -:O'zbekiston Axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi
78. -:Rossiya kiberjinoyatlarga qarshu kurashish davlat qo'mitasi
79. I:
80. S: Axborotdan oqilona foydalanish kodeksi nechanchi yil ishlab chiqilgan?
81. +:1973 yil
82. -:1980 yil
83. -:1991 yil
84. -:2002 yil
85. I:
86. S: Kompyuter bilan bog'liq falsafiy soha bo'lib, foydalanuvchilarning xatti-harakatlari, komyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko'rsatishini o'rgatadigan soha nima deb ataladi?
87. +:Kiberetika
88. -:Kiberhuquq
89. -:Kiberqoida
90. -:Kiberxavfsizlik
91. I:
92. S: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…
93. +:Kiberjinoyat
94. -:Kibersport
95. -:Kiberterror
96. -:Hakerlar uyushmasi
97. I:
98. S: Tarmoqlararo ekran paket filtrlari qaysi sathda ishlaydi?
99. +:Tarmoq sathida
100. -:Ilova sathida
101. -:Kanal sathida
102. -:Fizik sathida
103. I:
104. S: Tarmoqlararo ekran ekspert paketi filtrlari qaysi sathda ishlaydi?
105. +:Transport sathida
106. -:Ilova sathida
107. -:Kanal sathida
108. -:Fizik sathida
109. I:
110. S: Spam bilan kurashishning dasturiy uslubida nimalar ko’zda tutiladi?
111. +:Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida filtrlanib cheklanadi
112. -:Elektron pochta qutisiga kelib tushadigan spamlar me’yoriy xujjatlar asosida cheklanadi va bloklanadi
113. -:Elektron pochta qutisiga kelib tushadigan spamlar ommaviy ravishda cheklanadi
114. -:Elektron pochta qutisiga kelib spamlar mintaqaviy hududlarda cheklanadi
115. I:
116. S: Ma’lumotlarni yo’qolish sabab bo’luvchi tabiiy tahdidlarni ko’rsating
117. +:Zilzila, yong‘in, suv toshqini va hak
118. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
119. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
120. -:Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani
121. I:
122. S: Ma’lumotlarni tasodifiy sabablar tufayli yo’qolish sababini belgilang
123. +:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
124. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
125. -:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
126. -:Zilzila, yong‘in, suv toshqini va hak
127. I:
128. S: Ma’lumotlarni inson xatosi tufayli yo’qolish sababini belgilang.
129. +:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
130. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
131. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
132. -:Zilzila, yong‘in, suv toshqini va hak
133. I:
134. S: Ma’lumotlarni g’arazli hatti harakatlar yo’qolish sababini ko’rsating.
135. +:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
136. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
137. -:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
138. -:Zilzila, yong‘in, suv toshqini va hak
139. I:
140. S: Kompyuterda hodisalar haqidagi ma’lumot qayerda saqlanadi?
141. +:Hodisalar jurnaliga
142. -:Operativ xotiraga
143. -:Kesh xotiraga
144. -:Vaqtinchalik faylga
145. I:
146. S: Internet orqali masofada joylashgan kompyuterga yoki tarmoq resurslariga DoS hujumlari uyushtirilishi natijasida..
147. +:Foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan mahrum qilinadilar
148. -:Foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzg’unchilarga etkaziladi
149. -:Axborot tizimidagi ma’lumotlar bazalari o’g’irlanib ko’lga kiritilgach, ular yo’q qilinadilar
150. -:Foydalanuvchilar axborotlariga ruxsatsiz o’zgartirishlar kiritilib, ularning yaxlitligi buziladi
151. I:
152. S: Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo’naltirilgan buzg’unchi bu - ... .
153. +:Krakker
154. -:Hakker
155. -:Virus bot
156. -:Ishonchsiz dasturchi
157. I:
158. S: Antivirus dasturiy vositalari viruslarni tahlil qilishiga ko'ra necha turga bo'linadi?
159. +:2 turga: fayl Signaturaga va evristikaga asoslangan
160. -:2 turga: faol va passiv
161. -:2 turga: pulli va pulsiz
162. -:2 turga: litsenziyali va ochiq
163. I:
164. S: "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?
165. +:Foydalanish davrida maxfiylik kamayib boradi
166. -:Parolni esda saqlash kerak bo'ladi
167. -:Parolni almashtirish jarayoni murakkabligi
168. -:Parol uzunligi soni cheklangan
169. I:
170. S: Yaxlitlikni buzilishi bu - …
171. +:Soxtalashtirish va o’zgartirish
172. -:Ishonchsizlik va soxtalashtirish
173. -:Soxtalashtirish
174. -:Butunmaslik va yaxlitlanmaganlik
175. I:
176. S: Tarmoqda joylashgan fayllar va boshqa resurslardan foydalanishni taqdim etuvchi tarmoqdagi kompyuter nima?
177. +:Server
178. -:Bulutli tizim
179. -:Superkompyuter
180. -:Tarmoq
181. I:
182. S: Tahdid nima?
183. +:Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.
184. -:Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa
185. -:Bu riskni o‘zgartiradigan harakatlar bo‘lib
186. -:Bu noaniqlikning maqsadlarga ta’siri
187. I:
188. S: Risk nima?
189. +:Potensial kuchlanish yoki zarar
190. -:Potensial foyda yoki zarar
191. -:Tasodifiy taxdid
192. -:Katta yo‘qotish
193. I:
194. S: Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi?
195. +:Optik tolali
196. -:O’rama juft
197. -:Koaksial
198. -:Telefon kabeli
199. I:
200. S: Nima uchun autentifikatsiyalashda parol ko’p qo’llaniladi?
201. +:Sarf xarajati kam, almashtirish oson
202. -:Parolni eslab qolish oson
203. -:Parolni o’g’rishlash qiyin
204. -:Serverda parollarni saqlash oson
205. I:
206. S: Elektron xujjatlarni yo’q qilish usullari qaysilar?
207. +:Shredirlash, magnitsizlantirish, yanchish
208. -:Yoqish, ko’mish, yanchish
209. -:Shredirlash, yoqish, ko’mish
210. -:Kimyoviy usul, yoqish.
211. I:
212. S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?
213. +:Imzo qo‘yish va imzoni tekshirishdan
214. -:Faqat imzo qo‘yishdan
215. -:Faqat imzoni tekshirishdan
216. -:Kalitlarni taqsimlashdan
217. I:
218. S: Elektron pochtaga kirishda foydalanuvchi qanday autetntifikasiyalashdan o’tadi?
219. +:Parol asosida
220. -:Smart karta asosida
221. -:Biometrik asosida
222. -:Ikki tomonlama
223. I:
224. S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Jazolar bosqichiga to‘g‘ri ta’rif berilgan.
225. -: tashkilot o‘z siyosatini ishlab chiqishdan oldin o‘z aktivlari uchun risklarni baholashi shart
226. -: tashkilot o‘z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o‘rnatilish shart
227. -: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo‘shimcha kiritish jarayonida boshqaruvchi bo‘lishi shart
228. +: ma’lum tashkilotlarda tashkilotlarda qat’iy siyosatlar mavjud. Agar xodimlar ushbu siyosatlarga amal qilmasa, ularga qarshi bir qancha choralar qo‘llaniladi.
229. I:
230. S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Xodimlarni o‘rgatish bosqichiga to‘g‘ri ta’rif berilgan.
231. -: tashkilot o‘z siyosatini ishlab chiqishdan oldin o‘z aktivlari uchun risklarni baholashi shart
232. -: tashkilot o‘z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o‘rnatilish shart
233. -: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo‘shimcha kiritish jarayonida boshqaruvchi bo‘lishi shart
234. +: xodimlarga tashkilot xavfsizlik siyosati davomli ravishda o‘rgatilishi shart
235. I:
236. S: Galstuk babochka usuli nima?
237. +: Risklarni baholash usuli
238. -: Risklarni qabul qilish usuli
239. -: shifrlash algoritmi
240. -: Risklarni hosil qilish usuli.
241. I:
242. S: Lotin alifbosida DADA so‘zini 3 kalit bilan shifrlagandan so‘ng qaysi so‘z hosil bo‘ladi. A=0, B=1….Z=25.
243. +:GDGD
244. -: NANA
245. -: GPGP
246. -: FDFD
247. I:
248. S: Lotin alifbosida NON so‘zini 3 kalit bilan shifrlagandan so‘ng qaysi so‘z hosil bo‘ladi. A=0, B=1….Z=25.
249. -:GDGD
250. -: NANA
251. +: QRQ
252. -: FDFD
253. I:
254. S: Fizik to‘siqlarni o‘rnatish , Xavfsizlik qo‘riqchilarini ishga olish, Fizik qulflar qo‘yishni amalga oshirish qanday nazorat turiga kiradi?
255. +:Fizik nazorat
256. -: Texnik nazorat
257. -: Ma’muriy nazorat
258. -: Tashkiliy nazorat
259. I:
260. S: Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?
261. -: Fizik nazorat
262. +:Texnik nazorat
263. -: Ma’muriy nazorat
264. -: Tashkiliy nazorat
265. I:
266. S: Qoida va muolajalarni yaratish, Joylashuv arxitekturasini loyihalash, Xavfsizlik belgilari va ogohlantirish signallari, Ishchi joy xavfsizligini ta’minlash, Shaxs xavfsizligini ta’minlash amalga oshirish qanday nazorat turiga kiradi?
267. -: Fizik nazorat
268. -: Texnik nazorat
269. +: Ma’muriy nazorat
270. -: Tashkiliy nazorat
271. I:
272. S: Ikkilik sanoq tizimida qanday raqamlardan foydalanamiz?
273. +: Faqat 0 va 1
274. -: Faqat 1
275. -: Faqat 0
276. -: Barcha raqamlardan
277. I:
278. S: AES shifrlash algoritmi necha rounddan iborat
279. +: 10, 12, 14
280. -: 10,14,16
281. -: 12,14,16
282. -: 16
283. I:
284. S: Hodisalar daraxti usuli nima?
285. +: Risklarni baholash usuli
286. -: Risklarni qabul qilish usuli
287. -: shifrlash algoritmi
288. -: Risklarni hosil qilish usuli
289. I:
290. S: Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?
291. +:3 taga
292. -:4 taga
293. -:2 taga
294. -:5 taga

1. I:
2. S: WiMAX qanday simsiz tarmoq turiga kiradi.
3. +: Regional
4. -: Lokal
5. -: Global
6. -: Shaxsiy
7. I:
8. S: Wi-Fi necha Gs chastotali to'lqinda ishlaydi?
9. +: 2.4-5 Gs
10. -: 2.4-2.485 Gs
11. -: 1.5-11 Gs
12. -: 2.3-13.6 Gs
13. I:
14. S: Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi?
15. +: Onx458&hdsh)
16. +: 12456578
17. +: salomDunyo
18. +: Mashina777
19. I:
20. S: Parollash siyosatiga ko'ra parol tanlash shartlari qanday?
21. +: Kamida 8 belgi: katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. -: Kamida 8 belgi: katta va kichik xavflar, sonlar qo'llanishi kerak.
22. -: Kamida 6 belgi: katta xarflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak.
23. -: Kamida 6 belgi: katta va kichik xarflar, kamida bitta maxsus simvol qo'llanishi kerak.

1. Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

Foydalanishni boshqarish   
2. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?   
Xalqa   
3. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?   
Biometrik autentifikatsiya   
5. Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?   
Texnik nazorat   
6. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating   
Zilzila, yong‘in, suv toshqini va hak.   
7. Token, Smartkartalarda xavfsizlik tomonidan kamchiligi nimada?   
Qurilmalarni ishlab chiqarish murakkab jarayon   
8. Foydalanishni boshqarish –bu...   
Sub’ektni Sub’ektga ishlash qobilyatini aniqlashdir.   
9. Ro‘yxatdan o‘tish-bu…   
foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni   
10. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?   
Xavfsizlik siyosati ma’muri   
11. MD5, SHA1, SHA256, O‘z DSt 1106:2009- qanday algoritmlar deb ataladi?   
Shifrlash   
12. Shifr nima?   
Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm   
13. Ethernet kontsentratori qanday vazifani bajaradi?   
kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo‘naltirib beradi   
14. Tekstni boshqa tekst ichida ma’nosini yashirib keltirish nima deb ataladi?   
steganografiya   
15. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?   
{d, n} – yopiq, {e, n} – ochiq;   
16. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?   
1-2 jahon urushu davri   
17. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?   
Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi   
18. ……–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.   
Kiberxavfsizlik   
19. Kriptografiyaning asosiy maqsadi nima?   
maxfiylik, yaxlitlilikni ta’minlash   
20. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.   
ABAC

### 1. Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

 Foydalanishni boshqarish

### 2. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?

 Xalqa

### 3. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

 Biometrik autentifikatsiya

### 5. Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?

 Texnik nazorat

### 6. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating

 Zilzila, yong‘in, suv toshqini va hak.

### 9. Ro‘yxatdan o‘tish-bu…

 foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni

### 10. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

 Xavfsizlik siyosati ma’muri

### 12. Shifr nima?

 Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm

### 13. Ethernet kontsentratori qanday vazifani bajaradi?

 kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo‘naltirib beradi

### 14. Tekstni boshqa tekst ichida ma’nosini yashirib keltirish nima deb ataladi?

 steganografiya

### 15. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?

 {d, n} – yopiq, {e, n} – ochiq;

### 16. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

 1-2 jahon urushu davri

### 17. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

 Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

### 18. ……–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

 Kiberxavfsizlik

### 19. Kriptografiyaning asosiy maqsadi nima?

 maxfiylik, yaxlitlilikni ta’minlash

### 1. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.

 HandyBakcup

### 2. Makroviruslar nimalarni zararlaydi?

 Ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.

### 3. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….

 Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

### 4. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?

 Ruxsat berishga asoslangan siyosat

### 5. Nuqson atamasiga berilgan ma’noni ko‘rsating.

 Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi

### 6. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid Policy)

### 7. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuni qachon kuchga kirgan?

 1997 yil 24 aprel

### 8. Adware-zararli dastur vazifasi nimadan iborat?

 marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.

### 9. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

 Strukturalarni ruxsatsiz modifikatsiyalash

### 10. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?

 Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar

### 11. Fishing (ing. Fishing – baliq ovlash) bu…

 Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

### 12. Ma’lumotlarni zaxira nusxalash bu – …

 Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni.

### 13. ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.

 Risk monitoring

### 14. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.

 Recuva, R.saver

### 15. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

 Foydalanishni boshqarish

### 16. Kiberetika tushunchasi:

 Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

### 17. Rootkits-qanday zararli dastur?

 ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

### 18. "Fishing" tushunchasi:

 Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

### 19. Enterprise Information Security Policies, EISP-bu…

 Tashkilot axborot xavfsizligi siyosati

### 20. Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi?

 Razvedka hujumlari

### 1. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid Policy)

### 2. Spam bilan kurashishning dasturiy uslubida nimalar ko‘zda tutiladi?

 Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida filtrlanib cheklanadi.

### 3. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

 Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan

### 4. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud?

 detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar

### 5. "Axborotlashtirish to‘g‘risida"gi Qonunning maqsadi nimadan iborat?

 Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.

### 6. Ma’lumotlarni bloklarga bo‘lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?

 RAID 0

### 7. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

 Foydalanishni boshqarish

### 8. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.

 Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

### 9. Doktorlar, detektorlarga xos bo‘lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang.

 Faglar

### 10. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 1986

### 11. Rezident virus…

 tezkor xotirada saqlanadi

### 12. Zaiflik – bu…

 tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

### 13. Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi?

 Razvedka hujumlari

### 14. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

 Detektorlar

### 15. Makroviruslar nimalarni zararlaydi?

 Ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.

### 16. Texnik himoya vositаlаri – bu ...

 Texnik qurilmаlаr, komplekslаr yoki tizimlаr yordаmidа ob’ektni himoyalаshdir

### 17. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…

 Kiberjinoyat deb ataladi

### 19. Issue-Specific Security Policies, ISSP-bu…

 Muammofa qaratilgan xavfsizlik siyosati

### 20. Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.

qonunlar

### 1. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

 ABAC

### 2. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

 Xavfsizlik siyosati ma’muri

### 3. Kriptografiyaning asosiy maqsadi nima?

 maxfiylik, yaxlitlilikni ta’minlash

### 4. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?

 parol

### 5. Global simsiz tarmoqda qaysi standartlar ishlaydi?

 CDPD, 4G

### 6. Autentifikatsiya faktorlari nechta?

 3 ta

### 8. Kriptografiyada matn –bu..

 alifbo elementlarining tartiblangan to‘plami

### 9. Stenografiya ma’nosi qanday?

 sirli yozuv

### 11. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?

 Texnik vositalarning buzilishi va ishlamasligi

### 12. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

 Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

### 13. Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?

 Xesh funksiyalar

### 14. WiMAX qanday simsiz tarmoq turiga kiradi?

 Regional

### 15. Simmetrik shifrlashning noqulayligi – bu:

 Maxfiy kalitlar bilan ayirboshlash zaruriyatidir

### 16. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating

 Zilzila, yong‘in, suv toshqini va hak.

### 17. Ma’lumotlarni tasodifiy sabablar tufayli yo‘qolish sababini belgilang

 Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

### 18. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

 Biometrik autentifikatsiya

### 1. Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?

 3 taga

### 2. Kriptotizimga qo‘yiladigan umumiy talablardan biri nima?

 shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak

### 3. Autentifikatsiya faktorlari nechta?

 3 ta

### 4. Axborot xavfsizligining asosiy maqsadlaridan biri-bu…

 Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish

### 5. Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.

 Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

### 6. Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi?

 Optik tolali

### 7. Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?

 Xesh funksiyalar

### 8. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

 1-2 jahon urushu davri

### 9. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

 ABAC

### 10. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

 Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

### 11. Sub’ektga ma’lum vakolat va resurslarni berish muolajasi-bu:

 Avtorizatsiya

### 12. Kriptografiyaning asosiy maqsadi nima?

 maxfiylik, yaxlitlilikni ta’minlash

### 13. Identifikatsiya bu- …

 Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni

### 14. Fire Wall ning vazifasi...

 Tarmoqlar orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta’minlaydi

### 15. Kiberjinoyatchilik bu –. . .

 Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.

### 16. Berilgan ta’riflardan qaysi biri asimmetrik tizimlarga xos?

 Asimmetrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

### 17. Biometrik autentifikatsiyalashning avfzalliklari-bu:

 Biometrik parametrlarning noyobligi

### 18. "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?

 Foydalanish davrida maxfiylik kamayib boradi

### 19. Kriptografiyada kalitning vazifasi nima?

### 1. Spyware-qanday zararli dastur?

 Foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.

### 2. Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.

 Qonunlar

### 3. Adware-zararli dastur vazifasi nimadan iborat?

 marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.

### 4. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.

 HandyBakcup

### 5. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?

 RAID 5

### 6. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?

 Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar

### 7. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ... .

 Krakker

### 8. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?

 Paranoid siyosat

### 9. ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.

 Risk monitoring

### 10. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….

 Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

### 11. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko‘rsating?

 DDoS (Distributed Denial of Service) hujum

### 12. Kiberetika tushunchasi:

 Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

### 13. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.

 Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

### 14. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

 Foydalanishni boshqarish

### 15. Polimorf viruslar tushunchasi to‘g‘ri ko‘rsating.

 Viruslar turli ko‘rinishdagi shifrlangan viruslar bo‘lib, o‘zining ikkilik shaklini nusxadan-nusxaga o‘zgartirib boradi

### 16. Rezident virus…

 tezkor xotirada saqlanadi

### 17. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid Policy)

### 1. Kiberetika tushunchasi:

 Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

### 2. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

 Foydalanishni boshqarish

### 3. Doktorlar, detektorlarga xos bo‘lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang.

 Faglar

### 4. Zararli dasturlar qanday turlarga bo‘linadi?

 Dasturdagi zaifliklar(atayin qilingan) va zararli dasturlar(atayin qilingan)

### 5. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...

 Tamoqlararo ekranlarning o‘rnatilishi

### 6. Bag atamasini nima ma'noni beradi?

 Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo

### 7. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima deyiladi?

 Xavfsizlik siyosat

### 8. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.

 HandyBakcup

### 9. DIR viruslari nimani zararlaydi?

 FAT tarkibini zararlaydi

### 10. ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.

 Risk monitoring

### 11. Nuqson atamasiga berilgan ma’noni ko‘rsating.

 Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi

### 12. “Axborot olish kafolatlari va erkinligi to‘g‘risida”gi Qonunning 10-moddasi mazmuni qanday?

 Axborot manbaini oshkor etmaslik

### 13. Qaysi siyosat turli hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi?

 Maqbul foydalanish siyosati

### 14. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?

 Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar

### 15. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.

 Recuva, R.saver

### 16. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi?

 RAID 3

### 17. Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to‘liq tasavvurga ega shaxs kim deb ataladi?

 Xavfsizlik ma'muri (admin)

### 19. Ma’lumotlarni bloklarga bo‘lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?

 RAID 0

### 20. Qaysi siyosatda Adminstrator xavfsiz va zarur xizmatlarga indvidual ravishda ruxsat beradi?

 Extiyotkorlik siyosati

### 1. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating

 Zilzila, yong‘in, suv toshqini va hak.

### 2. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…

 login

### 3. Berilgan ta’riflardan qaysi biri asimmetrik tizimlarga xos?

 Asimmetrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

### 6. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

 1-2 jahon urushu davri

### 7. Wi-Fi necha Gs chastotali to‘lqinda ishlaydi?

 2.4-5 Gs

### 8. Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi.

 WEP, WPA, WPA2

### 11. Konfidentsiallikga to‘g‘ri ta’rif keltiring.

 axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

### 12. Autentifikatsiya nima?

 Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi

### 13. Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?

 Ma’lumotlar butunligi

### 14. ……–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

 Kiberxavfsizlik

### 15. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?

 {d, n} – yopiq, {e, n} – ochiq;

### 16. Kodlash nima?

 Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

### 17. Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq?

 simmetrik kriptotizimlar

### 18. Kriptografiyada kalitning vazifasi nima?

 Matnni shifrlash va shifrini ochish uchun kerakli axborot

### 19. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?

 Xalqa

### 20. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?

 Texnik vositalarning buzilishi va ishlamasligi

### 1. Konfidentsiallikga to‘g‘ri ta’rif keltiring.

 axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

### 2. Foydalanishni boshqarish –bu...

 Sub’ektni Ob’ektga ishlash qobilyatini aniqlashdir.

### 3. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?

 parol

### 4. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?

 Xalqa

### 5. Kodlash nima?

 Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

### 6. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?

 Yulduz

### 7. Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?

 Ma’lumotlar butunligi

### 8. Wi-Fi necha Gs chastotali to‘lqinda ishlaydi?

 2.4-5 Gs

### 9. Yaxlitlikni buzilishi bu - …

 Soxtalashtirish va o‘zgartirish

### 10. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

 1-2 jahon urushu davri

### 11. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

 Strukturalarni ruxsatsiz modifikatsiyalash

### 12. Kriptotizimga qo‘yiladigan umumiy talablardan biri nima?

 shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak

### 13. Risk nima?

 Potensial foyda yoki zarar

### 14. Assimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?

 Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun

### 15. Ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi?

 4 xil

### 16. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

 Xavfsizlik siyosati ma’muri

### 17. Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.

 Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.

### 3. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….

 Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

### 4. Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.

 Qonunlar

### 5. Rootkits-qanday zararli dastur?

 ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

### 6. Qaysi texnologiyada ma’lumotni ko‘plab nusxalari bir vaqtda bir necha disklarga yoziladi?

 RAID 1

### 7. "Axborotlashtirish to‘g‘risida"gi Qonunning maqsadi nimadan iborat?

 Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.

### 8. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid Policy)

### 10. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?

 Paranoid siyosat

### 11. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.

 "Sovuq saxiralash"

### 12. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

 Detektorlar

### 13. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ... .

 Krakker

### 14. "Fishing" tushunchasi:

 Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

### 15. O‘zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunning qaysi moddasi sabab qilib olingan?

 27(1)-modda. O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berishning alohida shartlari

### 16. Ma’lumotlarni zaxira nusxalash bu – …

 Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni.

### 17. Fishing (ing. Fishing – baliq ovlash) bu…

 Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

### 18. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 1986

### 19. "Backdoors"-qanday zararli dastur?

 zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

### 20. Kiberetika tushunchasi:

 Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

### 3. Ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi?

 4 xil

### 4. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

 Biometrik autentifikatsiya

### 5. Rol tushunchasiga ta’rif bering.

 Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin

### 6. Identifikatsiya bu- …

 Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni

### 7. Shifr nima?

 Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm

### 8. Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.

 Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

### 10. Stenografiya ma’nosi qanday?

 sirli yozuv

### 11. OSI modelida nechta sath mavjud?

 7 ta

### 12. Kriptografiyada kalitning vazifasi nima?

 Matnni shifrlash va shifrini ochish uchun kerakli axborot

### 13. Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi?

 Shaxsiy tarmoq

### 15. Risk nima?

 Potensial foyda yoki zarar

### 16. Kodlash nima?

 Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

### 17. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

 ABAC

### 18. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…

 login

### 19. Zamonaviy kriptografiya qanday bo‘limlardan iborat?

 Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish

### 1. Spam bilan kurashishning dasturiy uslubida nimalar ko‘zda tutiladi?

 Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida filtrlanib cheklanadi.

### 2. Ma’lumotlarni bloklarga bo‘lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?

 RAID 0

### 3. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.

 "Sovuq saxiralash"

### 4. Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to‘liq tasavvurga ega shaxs kim deb ataladi?

 Xavfsizlik ma'muri (admin)

### 5. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?

 RAID 5

### 6. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima deyiladi?

 Xavfsizlik siyosat

### 7. Fishing (ing. Fishing – baliq ovlash) bu…

 Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

### 8. Bag atamasini nima ma'noni beradi?

 Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo

### 9. "Backdoors"-qanday zararli dastur?

 zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

### 10. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 1986

### 11. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

 Detektorlar

### 12. Risk monitoringi ….. ni paydo bo‘lish imkoniyatini aniqlaydi.

 Yangi risklar

### 13. Ransomware qanday zarar keltiradi?

 mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi.

### 14. O‘zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunning qaysi moddasi sabab qilib olingan?

 27(1)-modda. O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berishning alohida shartlari

### 15. Texnik himoya vositаlаri – bu ...

 Texnik qurilmаlаr, komplekslаr yoki tizimlаr yordаmidа ob’ektni himoyalаshdir

### 17. Enterprise Information Security Policies, EISP-bu…

 Tashkilot axborot xavfsizligi siyosati

### 18. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?

 Paranoid siyosat

### 19. "Fishing" tushunchasi:

 Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

### 20. Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o‘z ichiga oladi?

 Xalqaro va milliy huquqiy me’yorlarni

### 1. "Fishing" tushunchasi:

 Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

### 2. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ... .

 Krakker

### 3. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?

 "Issiq zaxiralash"

### 4. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko‘rsating?

 DDoS (Distributed Denial of Service) hujum

### 5. Nuqson atamasiga berilgan ma’noni ko‘rsating.

 Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi

### 6. Risklarni identifikatsiya qilishdan maqsad nima?

 Potensial zarar yetkazadigan ehtimoliy insidentlarni prognozlash va bu zarar qay tarzda olinishi mumkinligi to‘g‘risida tasavvurga ega bo‘lish

### 7. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 1986

### 8. Rootkits-qanday zararli dastur?

 ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

### 9. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?

 Paranoid siyosat

### 10. Ko‘p platformali viruslar bu…

 Bir vaqtning o‘zida turli xildagi ob’ektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlaydi

### 11. “Axborot olish kafolatlari va erkinligi to‘g‘risida”gi Qonunning 10-moddasi mazmuni qanday?

 Axborot manbaini oshkor etmaslik

### 12. Risk monitoringi ….. ni paydo bo‘lish imkoniyatini aniqlaydi.

 Yangi risklar

### 13. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.

 Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

### 15. O‘zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunning qaysi moddasi sabab qilib olingan?

 27(1)-modda. O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berishning alohida shartlari

### 16. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?

 RAID 5

### 17. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

 Strukturalarni ruxsatsiz modifikatsiyalash

### 18. "Backdoors"-qanday zararli dastur?

 zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

### 19. Botnet-nima?

 internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi.

### 20. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

 Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan   
Windows OT lokal xavfsizlik siyosatini sozlash oynasiga o'tish uchun "Buyruqlar satri"ga quyidagi so'rovlardan qaysi biri kiritiladi?   
J:secpol.msc  
<http://fayllar.org>

2. Windows otda necha turdagi hodisa ro‘yxatga olinadi?  
  
1. Axborot xavfsizligining asosiy maqsadlaridan biri-bu…   
Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish   
2. Windows OTda necha turdagi hodisa ro‘yxatga olinadi?   
a) 5 ta   
3. Konfidentsiallikga to‘g‘ri ta’rif keltiring.   
a) axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;   
4. Kriptografiya faninining asosiy maqsadi nima?   
a) maxfiylik, yaxlitlilikni ta’minlash   
5. Kriptografiyada kalitning vazifasi nima?   
b) Matnni shifrlash va shifrini ochish uchun kerakli axborot   
6. Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq?   
a) simmetrik kriptotizimlar   
7. Autentifikatsiya nima?   
a) Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi   
8. Identifikatsiya bu- …   
a) Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni   
9. Kriptobardoshlilik deb nimaga aytilladi?   
a) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi   
10. Kriptografiyada matn –bu..   
a) alifbo elementlarining tartiblangan to‘plami

11. Kriptotizimga qo‘yiladigan umumiy talablardan biri nima?

a) shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak   
12. Berilgan ta’riflardan qaysi biri assimetrikrik tizimlarga xos?   
a) Assimetrikrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

13. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…

a) login   
14. Uning egasi haqiqiyligini aniqlash jarayonida matnhiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?   
a) parol   
15. Ro‘yxatdan o‘tish-bu…   
a) foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni   
16. Axborot qanday sifatlarga ega bo‘lishi kerak?   
a) ishonchli, qimmatli va to‘liq

17. Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish nima deb ataladi?

b) steganografiya   
18. Kriptografiya fan sifatida shakllanishida nechta davrlarga bo‘linadi?   
a) 4 ga

19. Shifrmatntni ochiq matntga akslantirish jarayoni nima deb ataladi?

a) Deshifrlash   
20. Risk-tushunchasi nima?   
a) Belgilangan sharoitda tahdidning manbalarga bo‘lishi mumkin bo‘lgan zarar yetkazilishini kutish   
21. Tahdid-tushunchasi nima?   
a) Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa   
22. Kodlash terminiga berilgan ta’rifni belgilang.   
a) Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir   
23. Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug‘ullanadi?   
b) Kriptoanaliz   
24. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?   
a) {d, n} – yopiq, {e, n} – ochiq;   
25. Zamonaviy kriptografiya qanday bo‘limlardan iborat?   
a) Simmetrik kriptotizimlar; Ochiq kalitli kriptotizimlar; Elektron raqamli imzo; Kalitlarni boshqarish   
26. Shifr nima?   
a) Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm   
27. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?   
b) Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi   
28. Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?   
c) Xesh funksiyalar   
29. Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...   
a) Avtorizatsiya   
30. Autentifikatsiya faktorlari nechta?   
b) 3 ta   
31. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?   
a) Biometrik autentifikatsiya   
32. Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini belgilaydigan atamani toping.   
b) Kriptobardoshlik   
33. Qog‘oz ma’lumotlarni yo‘q qilish odatda necha xil usuldan foydalaniladi?   
a) 4 xil   
34. Kiberjinoyat qanday turlarga bo‘linadi?   
a) Ichki va tashqi   
35. “Kiberxavfsizlik to‘g‘risida” Qonun qachon tasdiqlangan?   
a) 15.04.2022 y   
36. Kiberjinoyatchilik bu –. . .   
a) Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.   
37. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?   
d) Texnik vositalarning buzilishi va ishlamasligi   
38. Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?   
c) Ma’lumotlar butunligi   
39. Biometrik autentifikatsiyalashning avfzalliklari-bu:   
b) Biometrik parametrlarning noyobligi   
40. Simmetrik shifrlashning noqulayligi – bu:   
a) Maxfiy kalitlar bilan ayirboshlash zaruriyatidir   
41. Token, smartkartalarda xavfsizlik tomonidan kamchiligi nimada?   
a) Foydalanish davrida maxfiylik kamayib boradi   
b) Qurilmalarni ishlab chiqarish murakkab jarayon   
**c) Qurilmani yo‘qotilishi katta xavf olib kelishi mumkin**   
d) Qurilmani qalbakilashtirish oson

42. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating

a) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi   
**b) Zilzila, yong‘in, suv toshqini va hak.**   
c) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi   
d) Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani

43. Ma’lumotlarni tasodifiy sabablar tufayli yo‘qolish sababini belgilang

**a) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi**   
b) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi   
c) Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.   
d) Zilzila, yong‘in, suv toshqini va hak.

44. Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.

a) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi.   
**b) Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.**   
c) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi   
d) Zilzila, yong‘in, suv toshqini va hak.

45. "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?

a) Parolni esda saqlash kerak bo‘ladi.   
b) Parolni almashtirish jarayoni murakkabligi   
c) Parol uzunligi soni cheklangan   
**d) Foydalanish davrida maxfiylik kamayib boradi**

46. Nima uchun autentifikatsiyalashda parol ko‘p qo‘llaniladi?

**a) Sarf xarajati kam, almashtirish oson**   
b) Parolni foydalanubchi ishlab chiqadi   
c) Parolni o‘g‘rishlash qiyin   
d) Serverda parollar saqlanmaydi

47. Elektron xujjatlarni yo‘q qilish usullari qaysilar?

a) Yoqish, ko‘mish, yanchish   
**b) Shredirlash, magnitsizlantirish, yanchish**   
c) Shredirlash, yoqish, ko‘mish   
d) Kimyoviy usul, yoqish.

48. Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?

a) 4 taga   
b) 2 taga   
c) 5 taga   
**d) 3 taga**

49. Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi?

**a) Knx1@8&h**   
b) qwertyu   
c) salomDunyo   
d) Mashina505

50. Parollash siyosatiga ko‘ra parol tanlash shartlari qanday?

a) Kamida 7 belgi; katta va kichik xavflar, sonlar qo‘llanishi kerak.   
**b) Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo‘llanishi kerak.**   
c) Kamida 6 belgi; katta xarflar, sonlar , kamida bitta maxsus simvol qo‘llanishi kerak.   
d) Kamida 6 belgi; katta va kichik xarflar, kamida bitta maxsus simvol qo‘llanishi kerak.

51. MD5, SHA1, SHA256, O‘z DSt 1106:2009- qanday algoritmlar deb ataladi?

a) Kodlash   
**b) Xeshlash**   
c) Shifrlash   
d) Stenografiya

52. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

a) O‘rta asr davrida   
b) 15 asr davrida   
**c) 1-2 jahon urushu davri**   
d) 21 asr davrida

53. "Fishing" tushunchasi-bu…:

a) Kompyuter va kompyuter tarmoqlarida odamlarning etikasi   
b) Kompyuter, dasturlar va tarmoqlar xavfsizligi   
**c) Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi**   
d) Kompyuter tizimlariga ruxsatsiz ta’sir ko‘rsatish

54. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?

a) Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyot.   
b) Hisoblash tizimi xizmatlaridan foydalanish huqu kiberxavfsizlik qiga ega shaxs (shaxslar guruxi, tashkilot).   
**c) Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar**   
d) Ma’lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo‘ljallangan dasturiy va apparat vositalar

55. Axborot xavfsizligi timsollarini ko‘rsating.

a) Haker, Krakker   
**b) Alisa, Bob, Eva**   
c) Buzg‘unchi, hujumchi   
d) subyekt, user

56. Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.

**a) Qonunlar**   
b) Qarorlar   
c) Standartlar   
d) Farmonlar

57. Qaysi siyosat tizim resurslarini foydalanishda hech qanday cheklovlar qo‘ymaydi?

a) Ruxsat berishga asoslangan siyosat   
b) Paranoid siyosat   
c) Extiyotkorlik siyosati   
**d) Nomuntazam siyosat**

58. “Hаmmа nаrsа tа’qiqlаnаdi.” Bu qаysi xаvfsizlik siyosаtigа xos?

a) Ruxsаt berishgа аsoslаngаn siyosаt (Permissive Policy)   
**b) Pаrаnoid siyosаti (Pаrаnoid Policy)**   
c) Ehtiyotkorlik siyosаti (Prudent Policy)   
d) Nomuntаzаm siyosаt (Promiscuous Policy

59. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…

a) Kibersport deb ataladi   
b) Kiberterror deb ataladi   
**c) Kiberjinoyat deb ataladi**   
d) Hakerlar uyushmasi deyiladi

60. Qaysi siyosat turli hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi?

**a) Maqbul foydalanish siyosati**   
b) Paranoid siyosat   
c) Ruxsat berishga asoslangan siyosat   
d) Nomuntazam siyosat

61. Qaysi siyosatda Adminstrator xavfsiz va zarur xizmatlarga indvidual ravishda ruxsat beradi?

a) Paranoid siyosat   
b) Ruxsat berishga asoslangan siyosat   
c) Nomuntazam siyosat   
**d) Extiyotkorlik siyosati**

62. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?

a) Nomuntazam siyosat   
b) Paranoid siyosat   
**c) Ruxsat berishga asoslangan siyosat**   
d) Extiyotkorlik siyosati

63. Qaysi siyosatga ko‘ra hamma narsa taqiqlanadi?

a) Ruxsat berishga asoslangan siyosat   
b) Nomuntazam siyosat   
c) Extiyotkorlik siyosati   
**d) Paranoid siyosat**

64. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima deyiladi?

**a) Xavfsizlik siyosat**   
b) Standart   
c) Qaror   
d) Buyruq

65. Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to‘liq tasavvurga ega shaxs kim deb ataladi?

a) Xavfsizlik mutaxasisi   
b) Rahbar   
c) Foydalanuvchi   
**d) Xavfsizlik ma'muri (admin)**

66. Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o‘z ichiga oladi?

**a) Xalqaro va milliy huquqiy me’yorlarni**   
b) Tashkiliy va xalqaro me’yorlarni   
c) Ananaviy va korporativ me’yorlarni   
d) Davlat va nodavlat tashkilotlari me’yorlarni

67. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….

a) Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi   
b) Hamma narsa ta’qiqlanadi   
c) Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi   
**d) Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi**

68. ... - faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot.

**a) Parol**   
b) Login   
c) Maxfiy kalit   
d) Shifrlangan axborot

69. “Dasturiy ta’minotlar xavfsizligi” bilim sohasi - bu ...

**a) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.**   
**b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.**   
c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.   
d) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

70. “Jamoat xavfsizligi” bilim sohasi - bu …

**a) u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi.**   
b) tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini   
c) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi   
d) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

71. “Ma’lumotlar xavfsizligi” bilim sohasi - bu …

**a) ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.**   
b) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi   
c) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.   
d) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

72. “Tizim xavfsizligi” bilim sohasi - bu …

**a) tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi.**   
b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.   
c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.   
d) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

73. “Xodim xavfsizligi” tushunchasi- bu…

**a) Qandaydir jiddiy axborotdan foydalanish imkoniyatiga ega barcha xodimlarning kerakli avtorizatsiyaga va barcha kerakli ruxsatnomalarga egalik kafolatini ta’minlovchi usul.**   
b) Axborot tarmog‘ini ruxsatsiz foydalanishdan, me’yoriy harakatiga tasodifan aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.   
c) Destruktiv harakatlarga va yolg‘on axborotni zo‘rlab qabul qilinishiga olib keluvchi ishlanadigan va saqlanuvchi axborotdan ruxsatsiz foydalanishga urinishlarga kompyuter tizimining qarshi tura olish hususiyati.   
d) Korxona o‘z faoliyatini buzilishsiz va to‘xtalishsiz yurgiza oladigan vaqt bo‘yicha barqaror bashoratlanuvchi atrof-muhit holati.

74. “Yaxlitlik” atamasiga berilgan ta’rifni belgilang.

**a) Bu yozilgan va xabar qilingan ma’luotlarning haqiqiyligini, to‘g‘riligini, butunligini saqlash qobiliyati**   
b) Funksionala imkoniyatni o‘z vaqtida foydalanish   
c) Tizimning ruxsat berilgan foydalanish uchun ma’lumot tarqatishni cheklash   
d) Korxona o‘z faoliyatini buzilishsiz va to‘xtalishsiz yurgiza oladigan vaqt bo‘yicha barqaror bashoratlanuvchi atrof-muhit holati

75. ……–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

**a) Kiberxavfsizlik**   
b) Axborot xavfsizligi   
c) Kiberjtnoyatchilik   
d) Risklar

76. Assimetrikrik kriptotizimlarda axborotni shifrlashda va deshifrlash uchun qanday kalit ishlatiladi?

**a) Ikkita kalit: ochiq va yopiq**   
b) Bitta kalit   
c) Elektron raqamli imzo   
d) Foydalanuvchi identifikatori

77. Autentifikatsiya jarayoni qanday jarayon?

**a) obyekt yoki subyektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy axborotni tekshirish orqali asilligini aniqlash**   
b) axborot tizimlari obyekt va subyektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo‘yicha solishtirib uni aniqlash jarayoni   
c) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni   
d) foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni

78. Avtorizatsiya nima?

a) Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilarga tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni   
b) Subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim qilish jarayoni   
c) Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni   
d) Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilar

79. Axborot o‘lchovini kamayish tartibini to‘g‘ri tanlang

a) Terabayt,gigabayt,megabayt   
b) Bit,bayt,kilobayt,megabayt   
c) Gigabayt,megabayt,bayt   
d) Gigabayt,megabayat,terobayt

80. Axborot o‘lchovini o‘sish tartibini to‘g‘ri tanlang

a) Kilobayt,megabayt,gigabayt   
b) Bit,bayt,megabayt,kilobayt   
c) Gigabayt,megabayt,pikobayt   
d) Gigabayt,terabayt,pikobayt

81. Axborot xavfsizligi qanday asosiy xarakteristikalarga ega?

a) Butunlik, konfidentsiallik, foydalanuvchanlik   
b) Butunlik, himoya, ishonchlilikni o‘rganib chiqishlilik   
c) Konfidentsiallik, foydalana olishlik   
d) Himoyalanganlik, ishonchlilik, butunlik

82. Axborot xavfsizligining huquqiy ta'minotiga nimalar kiradi?

a) Qonunlar, aktlar, me'yoriy-huquqiy hujjatlar, qoidalar, yo‘riqnomalar, qo‘llanmalar majmui   
b) Qoidalar yo‘riqnomalar, tizim arxetikturasi, xodimlar malakasi, yangi qoidalar, yangi yo‘riqnomalar, qo‘llanmalar majmui   
c) Qoidalar, yo‘riqnomalar, tizim strukturasi, dasturiy ta’minot   
d) Himoya tizimini loyihalash, nazorat usullari

83. "Barcha xizmatlar blokirovka qilingandan so‘ng bog‘lanadi". -Bu qaysi xavfsizlik siyosatiga hos?

a) Ehtiyotkorlik siyosati (Prudent Policy)   
b) Nomuntazam siyosat (Promiscuous Policy)   
c) Paranoid siyosati (Paranoid Policy)   
d) Ruxsat berishga asoslangan siyosat (Permissive Policy)

84. Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo‘linadi?

a) Blokli va oqimli   
b) DES va oqimli   
c) Feystel va Verman   
d) SP− tarmoq va IP

85. BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?

a) AES, Serpent, Twofish   
b) Pleyfer, Sezar   
c) DES, sezar, Futurama   
d) AES, Serpent, Twofish, Triple DES, GOST 28147-89

86. Blokli shifrlash tushunchasi nima?

a) shifrlanadigan matn blokiga qo‘llaniladigan asosiy akslantirish   
b) murakkab bo‘lmagan kriptografik akslantirish   
c) axborot simvollarini boshqa alfavit simvollari bilan almashtirish   
d) ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi

87. Elektron pochtaga kirishda foydalanuvchi qanday autetntifikasiyalashdan o‘tadi?

a) Parol asosida   
b) Smart karta asosida   
c) Biometrik asosida   
d) Ikki tomonlama

88. Elektron raqamli imzo - bu …

a) xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimcha   
b) matnni shifrlash va shifrini ochish uchun kerakli axborot   
c) axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam   
d) kalit axborotni shifrlovchi kalitlar

89. Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?

a) Imzo qo‘yish va imzoni tekshirishdan   
b) Faqat imzo qo‘yishdan   
c) Faqat imzoni tekshirishdan   
d) Kalitlarni taqsimlashdan

90. Elektron raqamli imzo kalitlari ro‘yxatga olish qaysi tashkilot tomonidan bajariladi

a) Sertifikatlari roʻyxatga olish markazlari   
b) Tegishli Vazirliklar   
c) Axborot xavfsizligi markazlari   
d) Davlat Hokimiyati

91. Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima?

a) Autentifikatsiya   
b) Identifikatsiya   
c) Avtorizatsiya   
d) Ma’murlash

92. Kriptografiyada kalit – bu …

a) Matnni shifrlash va shifrini ochish uchun kerakli axborot   
b) Bir qancha kalitlar yig‘indisi   
c) Axborotli kalitlar to‘plami   
d) Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

93. Kiberetika tushunchasi-bu…

a) Kompyuter va kompyuter tarmoqlarida odamlarning etikasi   
b) Kompyuter, dasturlar va tarmoqlar xavfsizligi   
c) Kompyuter tizimlariga ruxsatsiz ta’sir ko‘rsatish   
d) Tashkilot va odamlarning mahsus va shahsiy ma’lumotlarini olishka qaratilgan internet-atakasi

94. Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi?

a) tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi   
b) tashkilot xodimlari himoyasini ta’minlaydi   
c) tashkilot axborotlari va binolarining himoyasini ta’minlaydi   
d) tashkilot omborini va axborotlari himoyasini ta’minlaydi

95. Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda qo‘llaniladi?

a) ochiq kalitlar   
b) yopiq kalitlar   
c) seans kalitlari   
d) Barcha tutdagi kalitlar

96. Kriptografiyada "alifbo" deganda nima tushuniladi?

a) axborotni ifodalashda ishlatiluvchi bilgilarning chekli to‘plami tushuniladi   
b) matnni shifrlash va shifrini ochish uchun kerakli axborot   
c) xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimcha   
d) alfavit elementlaridan tartiblangan nabor

97. O‘zbekistonda masofadan elektron raqamli imzo olish uchun qaysi internet manzilga murojaat qilinadi?

a) e-imzo.uz   
b) elektron-imzo.uz   
c) imzo.uz   
d) eri.uz

98. Oqimli shifrlashning mohiyati nimada?

a) Oqimli shifrlash birinchi navbatda axborotni bloklarga bo‘lishning imkoni bo‘lmagan hollarda zarur,   
b) Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo‘natish uchun oqimli shifrlash zarur,   
c) Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo‘yicha shifrlaydi   
d) Oqimli shifrlash birinchi navbatda axborotni bloklarga bo‘lishning imkoni bo‘lgan hollarda zarur,

99. RSA algoritmi qanday jarayonlardan tashkil topgan?

a) Kalitni generatsiyalash; Shifrlash; Deshifrlash.   
b) Shifrlash; Imzoni tekshirish; Deshifrlash   
c) Kalitni generatsiyalash; imzolash; Deshifrlash.   
d) Imzoni tekshirish ; Shifrlash; Deshifrlash.

100. Shaxsning, o‘zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, axborot-kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu?

a) login   
b) parol   
c) identifikatsiya   
d) maxfiy maydon

101. Shifrlash qanday jarayon?

a) akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi   
b) kalit asosida shifrmatn ochiq matnga akslantiriladi   
c) shifrlashga teskari jarayon   
d) almashtirish jarayoni bo‘lib: ochiq matn deb nomlanadigan matn o‘girilgan holatga almashtiriladi

102. Kichik xajmdagi xotira va hisoblash imkoniyatiga ega bo‘lgan, o‘zida parol yoki kalitni saqlovchi qurilma nima deb ataladi?

a) Token, Smartkarta   
b) Chip   
c) Fleshka   
d) Disk

103. Cisco tashkiloti “kiberxavfsizlik” atamasiga qanday ta’rif bergan?

a) Kiberxavfsizlik - tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti   
b) Hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan   
c) Bu yozilgan va xabar qilingan ma’luotlarning haqiqiyligini, to‘g‘riligini, butunligini saqlash qobiliyati   
d) Ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.

104. Foydalanuvchanlik-bu…

a) avtorizatsiyalangan mantiqiy obyekt so‘rovi bo‘yicha axborotning tayyorlik va foydalanuvchanlik holatida bo‘lishi xususiyati   
b) axborotning buzilmagan ko‘rinishida (axborotning qandaydir qayd etilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati   
c) axborot yoki uni eltuvchisining shunday holatiki, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi   
d) potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi

105. Kiberxavfsizlik bilim sohasi nechta bilim sohasini o‘z ichiga oladi?

a) 8 ta   
b) 7 ta   
c) 6 ta   
d) 5 ta

106. Ijtimoiy (sotsial) injineriya-bu…

a) turli psixologik usullar va firibgarlik amaliyotining to‘plami, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olish   
b) Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish   
c) axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi   
d) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

107. Kiberxavfsizlik arxitekturasi nechta sathga ajratiladi?

a) 3ta   
b) 2 ta   
c) 4 ta   
d) 5 ta

108. Tashkilot axborot xavfsizligi siyosati-bu…

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.   
b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.   
c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.   
d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

109. Muammoga qaratilgan xavfsizlik siyosatlari …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.   
**b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.**   
c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.   
d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

110. Tizimga qaratilgan xavfsizlik siyosatlari …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.   
b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.   
**c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.**   
d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

111. Internetdan foydalanish siyosati. …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.   
b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.   
c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.   
**d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.**

112. Ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o‘zgartirishlar oilasi-…

**a) Kriptotizim**   
b) Deshifrlash   
c) Rasshifrovkalash   
d) Shifrlash

113. O‘zgartirishlar oilasidan birini tanlashni ta’minlovchi kriptografik algoritmning qandaydir parametrlarining muayyan qiymati-…

a) Kriptotizim   
**b) Kalit**   
c) Rasshifrovkalash   
d) Shifrlash

114. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuning maqsadi nimadan iborat?

a) Har kimning axborotni erkin va moneliksiz izlash, olish, tadqiq etish, uzatish hamda tarqatishga doir konstitutsiyaviy huquqini amalga oshirish jarayonida yuzaga keladigan munosabatlarni tartibga solish   
b) Axborotlarni maxfiylashtirish va maxfiylikdan chiqarish ushbu Qonunga hamda o‘zbekiston Respublikasi Vazirlar Mahkamasi tasdiqlaydigan ma’lumotlarning maxfiylik darajasini aniqlash va belgilash   
c) Shaxsga doir ma’lumotlar sohasidagi munosabatlarni tartibga solish.   
d) Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.

115. "Axborotlashtirish to‘g‘risida"gi Qonunning maqsadi nimadan iborat?

a) Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.   
b) Shaxsga doir ma’lumotlar sohasidagi munosabatlarni tartibga solish.   
c) Har kimning axborotni erkin va moneliksiz izlash, olish, tadqiq etish, uzatish hamda tarqatishga doir konstitutsiyaviy huquqini amalga oshirish jarayonida yuzaga keladigan munosabatlarni tartibga solish   
d) Axborotlarni maxfiylashtirish va maxfiylikdan chiqarish ushbu Qonunga hamda o‘zbekiston Respublikasi Vazirlar Mahkamasi tasdiqlaydigan ma’lumotlarning maxfiylik darajasini aniqlash va belgilash

116. "Backdoors"-qanday zararli dastur?

a) zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, masalan, administrator parolisiz imtiyozga ega bo‘lish   
b) foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod   
c) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi   
d) marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot

117. .... – o‘zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma’lumoti va xavfsizlik algoritmlarini saqlaydi.

a) Sim karta   
b) Token   
c) Smart karta   
d) Elektron raqamli imzo

118. .... kompyuter tarmoqlari bo‘yicha tarqalib, kompyuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o‘zining nusxasini qoldiradi.

a) “Chuvalchang” va replikatorli virus   
b) Kvazivirus va troyan virus   
c) Troyan dasturi   
d) Mantiqiy bomba

119. “Aloqa xavfsizligi” bilim sohasi - bu …

a) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.   
b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.   
c) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.   
d) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

120. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

a) Foydalanishni boshqarish   
b) Tarmoqni loyihalash   
c) Foydalanish   
d) Identifikatsiya

121. “Inson xavfsizligi” bilim sohasi - bu …

a) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi   
b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi   
c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.   
d) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi

122. “Tashkil etuvchilar xavfsizligi” - bu …

a) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi   
b) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi   
c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi   
d) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi

123. “Tashkilot xavfsizligi” bilim sohasi - bu …

a) tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini   
b) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi   
c) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi   
d) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi

124. …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.

a) UDP   
b) HTTP   
c) TCP   
d) FTP

125. ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.

a) TCP   
b) IP   
c) HTTP   
d) FTP

126. Access control list va Capability list bu nimaning asosiy elementi hisoblanadi?

a) Lampson matritsasining   
b) XASML standartining   
c) Role-based access control RBACning   
d) Attribute based access control (ABAC)ning

127. “Adware” zararli dastur xususiyati nimadan iborat?

a) marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.   
b) foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.   
c) bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi.   
d) o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi

128. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?

a) "Issiq zaxiralash"   
b) "Sovuq saxiralash"   
c) "Iliq saxiralash"   
d) "To‘liq zaxiralash"

129. Qaysi zaxiralash usuli offlayn zaxiralash deb ham atalib, tizim ishlamay turganida yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi?

a) "Sovuq saxiralash"   
b) "Issiq zaxiralash"   
c) "Iliq saxiralash"   
d) "To‘liq zaxiralash"

130. Qaysi zaxiralashda tizim muntazam yangilanishni amalga oshirish uchun tarmoqqa bog‘lanishi kerak bo‘ladi?

a) "Iliq saxiralash"   
b) "Sovuq saxiralash"   
c) "Issiq zaxiralash"   
d) "To‘liq zaxiralash"

131. Agar RSA algotirmida e-ochiq kalitni, d-maxfiy kalitni, n-modul ifodalasa, qaysi formula deshifrlashni ifodalaydi?

a) M = C^d mod n;   
b) C = M^d mod n;   
c) C = M^ed mod n;   
d) M = C^e mod n;

132. Agar RSA algotirmida e-ochiq kalitni, d-maxfiy kalitni, n-modul , qaysi formula shifrlashni ifodalaydi?

a) C = M^e mod n;   
b) C = M^d mod n;   
c) C = M^ed mod n;   
d) M = C^e mod n;

133. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...

a) Tamoqlararo ekranlarning o‘rnatilishi   
b) Tashkiliy ishlarni bajarilishi   
c) Globol tarmoqdan uzib qo‘yish   
d) Aloqa kanallarida optik toladan foydalanish

134. Akslantirish tushunchasi deb nimaga aytiladi?

a) 1-to‘plamli elementlariga 2-to‘plam elementalriga mos bo‘lishiga   
b) 1-to‘plamli elementlariga 2-to‘plam elementalrini qarama-qarshiligiga   
c) har bir elementni o‘ziga ko‘payimasiga   
d) agar birinchi va ikinchi to‘plam bir qiymatga ega bo‘lmasa

135. Antivirus dasturiy vositalari viruslarni tahlil qilishiga ko‘ra necha turga bo‘linadi?

a) 2 turga fayl signaturaga va tahlilga asoslangan   
b) 2 turga faol va passiv   
c) 2 turga pulli va pulsiz   
d) 2 turga litsenziyali va ochiq

136. Antivirus dasturlarini ko‘rsating.

a) Drweb, Nod32, Kaspersky   
b) arj, rar, pkzip, pkunzip   
c) winrar, winzip, winarj   
d) pak, lha

137. Antiviruslar viruslarni asosan qanday usulda aniqlaydi?

a) Signaturaga asoslangan   
b) Anomaliyaga asoslangan   
c) O‘zgarishni aniqlashga asoslangan   
d) Defragmentatsiya qilish

138. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud.

a) detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar   
b) detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar   
c) vaktsinalar, privivkalar, revizorlar, matnhiruvchilar   
d) privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar

139. AQShning axborotni shifrlash standartini keltirilgan javobni ko‘rsating?

a) DES(Data Encryption Standart)   
b) RSA (Rivest, Shamir ва Adleman)   
c) AES (Advanced Encryption Standart)   
d) Aniq standart ishlatilmaydi

140. Assimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?

a) shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun   
b) shifrlash, deshifrlash, kalit generatsiyalash   
c) ERI hosil qilsih, maxfiylikni ta’minlash, kalitlar almashish uchun   
d) shifrlash, deshifrlash, kalitlar boshqarish uchun

141. Assimmetrik kriptotizimlarda axborotni shifrlashda va deshifrlash uchun nechta kalit ishlatiladi?

a) Ikkita kalit   
b) Bitta kalit   
c) Uchta kalit   
d) Foydalanuvchi identifikatori

142. Asosan tarmoq, tizim va tashkilot haqidagi axborotni olish maqasadida amalga oshiriladigan tarmoq hujumini belgilang.

a) Razvedka hujumlari   
b) Kirish hujumlari   
c) DOS hujumi   
d) Zararli hujumlar

143. Atribute based access control ABAC usuli attributlari qaysilar?

a) Foydalanuvchi attributlari   
b) Asosiy va qo‘shimcha atributlar   
c) Tizim attributlari, server atributlari   
d) Ichki va tashqi attributlar

144. Autentifikatsiyaga ta'rif qaysi javobda keltirilgan?

a) Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi   
b) Tizim meyoriy va g‘ayritabiiy hollarda rejalashtirilgandek o‘zini tutishligi holati   
c) Istalgan vaqtda dastur majmuasining mumkinligini kafolati   
d) Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi

145. Avtorizatsiya qanday jarayon?

a) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni   
b) axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo‘yicha solishtirib uni aniqlash jarayoni   
c) obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash.   
d) foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni

146. Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?

a) Korporativ va umumfoydalanuvchi   
b) Regional, korporativ   
c) Lokal, global   
d) Shaharlararo, lokal, global

147. Axborot paketlarini qachon ushlab qolish mumkin?

a) Aloqa kanallari orqali uzatishda   
b) Xotira qurilmalarida saqlanayotganda   
c) Kompyuter ishga tushganda   
d) Ma’lumotlar nusxalanayotganda

148. Axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi nima deb ataladi?

a) Axborot resursi   
b) Axborot xavfsizligi   
c) Ma'lumotlar bazasi   
d) Axborot tizimlari

149. Axborot tizimiga ta’rif bering.

a) Qo‘yilgan maqsadga erishish yo‘lida axborotlarni olish, qayta ishlash, va uzatish uchun usullar, vositalar va xodimlar jamlanmasi   
b) Material olamda axborot almashinuvining yuzaga kelishini ta’minlovchi axborot uzatuvchi, aloqa kanallari, qabul qilgich vositalar jamlanmasi   
c) Qo‘yilgan maqsadga erishish yo‘lida o‘zaro birlashtirilgan va ayni vaqtda yagona deb qaraluvchi elementlar to‘plami   
d) Ishlab chiqarish jarayonida insonlarning umumiy munosabatlarini ifodalovchi vositlar to‘plami

150. Axborot xavfsizligi siyoatining necha xil turi bor?

a) 3   
b) 4   
c) 5   
d) 2

151. Axborot xavfsizligi siyosati –bu …

a) tashkilot o‘z faoliyatida rioya qiladigan axborot xavfsizligi sohasidagi hujjatlangan qoidalar, muolajalar, amaliy usullar yoki amal qilinadigan prinsiplar majmui sanalib, u asosida tashkilotda axborot xavfsizligi ta’minlanadi   
b) mavjud tahdidni amalga oshirilgan ko‘rinishi bo‘lib, bunda kutilgan tahdid amalga oshiriladi   
c) mavjud bo‘lgan zaiflik natijasida bo‘lishi mumkin bo‘lgan hujum turi bo‘lib, ular asosan tizimni kamchiliklarini o‘rganish natijasida kelib chiqadi   
d) tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

152. 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 muhumligi 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

153. Axborot xavfsizligini ta'minlovchi choralarni ko‘rsating?

a) 1-huquqiy, 2-tashkiliy-ma'muriy, 3-dasturiy-texnik   
b) 1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy   
c) 1-amaliy, 2-tashkiliy-ma'muriy, 3-huquqiy   
d) 1-apparat, 2-texnikaviy, 3-huquqiy

154. Axborotdan oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan?

a) AQSH sog‘liqni saqlash va insonlarga xizmat ko‘rsatish vazirligi   
b) AQSH Mudofaa vazirligi   
c) O‘zbekiston Axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi   
d) Rossiya kiberjinoyatlarga qarshu kurashish davlat qo‘mitasi

155. Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?

a) USB fleshka, CD va DVD disklar   
b) Qattiq disklar va CDROM   
c) CD va DVD, kesh xotira   
d) Qattiq disklar va DVDROM

156. Axborotni himoyalash uchun ... usullari qo‘llaniladi.

a) kodlashtirish, kriptografiya, stegonografiya   
b) shifrlash va kriptografiya, maxsus yozilgan kod   
c) Stegonografiya, kriptografiya, orfografiya   
d) Kriptoanaliz, kodlashtirish, zahiralash

157. Axborotning buzilishi yoki yo‘qotilishi xavfiga olib keluvchi himoyalanuvchi obyektga qarshi qilingan xarakatlar qanday nomlanadi?

a) Tahdid   
b) Zaiflik   
c) Hujum   
d) Butunlik

158. Axborotning eng kichik o‘lchov birligi nima?

a) bit   
b) kilobayt   
c) bayt   
d) kilobit

159. Axbоrоt tizimlari xavfsizligining auditi-bu…

a) Axborot tizimlarining himoyalanishining joriy holati, tizim haqida obyektiv ma’lumotlarni olish va baholash   
b) Ma`lumоtlarini tahlillash va chоra ko‘rishni tizim haqida subyektiv ma’lumotlarni olish va baholashni tahlil qiladi   
c) Ma`lumоtlarini tarqatish va boshqarish   
d) Axbоrоtni yig‘ish va korxona tarmog‘ini tahlillash

160. TrueCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?

a) AES, Serpent va Twofish   
b) Serpent, RSA   
c) El-Gamal, Twofish   
d) DES

161. "Bag" atamasini nima ma'noni beradi?

a) Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo   
b) Mualliflik huquqini buzilishi   
c) Dasturlardagi ortiqcha reklamalar   
d) Autentifikatsiya jarayonini buzish

162. "Barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti".- Bular tarmoqning qaysi sathiga kiradi?

a) Fizik sath (physical)   
b) Tarmoq sathi   
c) Amaliy sath   
d) Tadbiqiy sath

163. Bell-LaPadula (BLP) modeli -bu..

a) Bu hukumat va harbiy dasturlarda kirishni boshqarishni kuchaytirish uchun ishlatiladigan avtomatlashgan modeli   
b) Axborlarni nazoratlovchi model   
c) Foydalanuvchilarni ro‘yxatga olish , nazoratlash va tahlil qiluvchi model   
d) Tarmoq boshqarish va tahlil qiluvchi model

164. Bell-LaPadula axborot xavfsizligida axborotni qaysi parametrini ta'minlash uchun xizmat qiladi?

a) Konfidentsiallikni   
b) Yaxlitlikni   
c) Maxfiylikni   
d) O‘zgarmaslikni

165. Biba modeli obyektni qaysi xusuiyatiga e'tibor qaratilgan?

a) Yaxlitligi   
b) Maxfiyligi   
c) Xavfsizligi   
d) Konfidentsialligi

166. BiBa modeli qaysi modelning keygaytirilgan varianti hisoblanadi?

a) Bell-Lapadula modeli   
b) RBAC   
c) MAC   
d) ABAC

167. Biometrik parametrlarda xavfsizlik tomonidan kamchiligi nimadan iborat?

a) ID ni almashtirish murakkabligi   
b) Foydalanish davrida maxfiylik kamayib boradi   
c) Qalbakilashtirish oson   
d) Parol va PIN kod ishlatilmasligi

168. Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang.

a) Shaxsiy simsiz tarmoq   
b) Lokal simsiz tarmoq   
c) Regional simsiz tarmoq   
d) Global simsiz tarmoq

169. Botnet-nima?

a) internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi   
b) zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi   
c) zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish.   
d) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

170. …-bu so‘z ingliz tilidan olingan bo‘lib- yorib tashlash, chopish, buzish degan ma’nolarni anglatadi. Ular xaddan ziyod malakali va bilimli, axborot texnologiyalarini puxta biluvchi insondir.-Yuqoridagi fikr kim to‘g‘risida ta’rif berilgan?

a) Xaker   
b) Dasturchi   
c) Tarmoq josusi   
d) Administrator

171. Bulutli texnologiyalarda PaaS nimani ifodalaydi?

a) Platforma sifatida   
b) Servis sifatida   
c) Ma'lumot sifatida   
d) Prizentatsiya sifatida

172. GSM, GPRS, EDGE, HSPA+, LTE standartida ishlovchi simsiz tarmoq turini aniqlang.

a) Global simsiz tarmoq   
b) Shaxsiy simsiz tarmoq   
c) Lokal simsiz tarmoq   
d) Regional simsiz tarmoq

173. Cloud Computing texnologiyasi nechta katta turga ajratiladi?

a) 3 turga   
b) 2 turga   
c) 4 turga   
d) 5 turga

174. Dastur kodini tashkil qilish yondashuviga ko‘ra viruslar turlari?

a) Shifrlangan, shifrlanmagan, polimorf   
b) Dasturiy, yuklanuvchi, makroviruslar, multiplatformali viruslar   
c) Rezident, norezident   
d) Virus parazit, virus cherv

175. Dasturiy shifrlash vositalari necha turga bo‘linadi?

a) 4   
b) 3   
c) 5   
d) 6

176. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ...

a) Krakker   
b) Hakker   
c) Virus bot   
d) Ishonchsiz dasturchi

177. DIR viruslari nimani zararlaydi?

a) FAT tarkibini zararlaydi   
b) com, exe kabi turli fayllarni zararlaydi   
c) yuklovchi dasturlarni zararlaydi   
d) Operatsion tizimdagi sonfig.sys faylni zararlaydi

178. Diskni shifrlash nima uchun amalga oshiriladi?

a) Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi   
b) Xabarni yashirish uchun amalga oshiriladi   
c) Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi   
d) Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi

179. Doktorlar, detektorlarga xos bo‘lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang.

a) Faglar   
b) Detektorlar   
c) Vaksinalar   
d) Privivka

180. Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi.

a) Fizik sath (physical)   
b) Kanal sath (data link)i   
c) Tarmoq sathi   
d) Transport sathi

181. Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?

a) raqamli imzoni shakllantirish va tekshirish muolajasi   
b) raqamli imzoni hisoblash muolajasi   
c) raqamli imzoni hisoblash va tekshirish muolajasi   
d) raqamli imzoni shakllantirish muolajasi

182. Eng ko‘p axborot xavfsizligini buzilish xolati-bu:

a) Tarmoqda ruxsatsiz ichki foydalanish   
b) Tizimni loyihalash xatolaridan foydalanish   
c) Tashqi tarmoq resursiga ulanish   
d) Simsiz tarmoqqa ulanish

183. Enterprise Information Security Policies, EISP-bu…

a) Tashkilot axborot xavfsizligi siyosati   
b) Muammofa qaratilgan xavfsizlik siyosati   
c) Tizimga qaratilgan xavfizlik siyosati   
d) Maqbul foydalanish siyosati

184. Ethernet konsentratori(hub) qanday vazifani bajaradi?

a) kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo‘naltirib beradi   
b) kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo‘naltirib beradi   
c) kompyuterdan kelayotgan axborotni xalqa bo‘ylab joylashgan keyingi kompyuterga   
d) tarmoqning ikki segmentini bir biriga ulaydi

185. Faol hujum turi deb nimaga aytiladi?

a) Maxfiy uzatish jarayonini uzib qo‘yish, modifikatsiyalash, qalbaki shifr ma’lumotlar tayyorlash harakatlaridan iborat jarayon   
b) Maxfiy ma’lumotni aloqa tarmog‘ida uzatilayotganda eshitish, tahrir qilish, yozib olish   
c) harakatlaridan iborat uzatilalayotgan ma’lumotni qabul qiluvchiga o‘zgartirishsiz yetkazish jarayoni   
d) Ma’lumotga o‘zgartirish kiritmay uni kuzatish jarayoni   
e) Sust hujumdan farq qilmaydigan jarayon

186. Faollashish prinspiga ko‘ra viruslar turlari?

a) Rezident, Norezident   
b) Dasturiy, Makroviruslar, multiplatformali viruslar   
c) Virus parazit, Virus cherv   
d) Shifrlangan, shifrlanmagan, Polimorf

187. Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o‘zgarib turadigan parol nima deyiladi?

a) One-time password (OTP)   
b) Only password (OP)   
c) First Password (FP)   
d) Primary Password (PP)

188. Faqat ma’lum hizmatlar /hujumlar/harakatlar bloklanadi. Bu qaysi xavfsizlik siyosatiga hos?

a) Ruxsat berishga asoslangan siyosat (Permissive Policy)   
b) Ehtiyotkorlik siyosati (Prudent Policy)   
c) Nomuntazam siyosat (Promiscuous Policy)   
d) Paranoid siyosati (Paranoid Policy)

189. Fire Wall ning vazifasi...

a) Tarmoqlar orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta`minlaydi   
b) kompyuterlar tizimi xavfsizligini ta`minlaydi   
c) Ikkita kompyuter o‘rtasida aloqa o‘rnatish jarayonida Internet tarmog‘i orasida xavfsizlikni ta`minlaydi   
d) uy tarmog‘i orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta`minlaydi

190. Fizik to‘siqlarni o‘rnatish , Xavfsizlik qo‘riqchilarini ishga olish, Fizik qulflar qo‘yishni amalga oshirish qanday nazorat turiga kiradi?

a) Fizik nazorat   
b) Texnik nazorat   
c) Ma’muriy nazorat   
d) Tashkiliy nazorat

191. Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi?

a) 2 taga   
b) 4 taga   
c) 3 taga   
d) 5 taga

192. Fizik xavfsizlikni nazoratlashga nimalar kiradi?

a) Binoga to‘siqlar qo‘yish, eshikka qulflar o‘rnatish, xavfsizlik xodimlarini ishga olish.   
b) Kompyuterlarga antivirus o‘rnatish, serverlarni ko‘paytirish, to‘siqlarni o‘rnatish   
c) Hujjatlarni tashkillashtirish, xodimlarni o‘qitish,qulflarni o‘rnatish   
d) Ruxsatni nazoratlash,shaxs xavfsizligini ta’minlash,muhitni nazoratlash

193. Foydalanish huquqini cheklovchi matritsa modeli bu...

a) Bella La-Padulla modeli   
b) Dening modeli   
c) Landver modeli   
d) Huquqlarni cheklovchi model

194. Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari-bu…

a) Foydalanuvchanligi   
b) Ma’lumotlar butunligi   
c) Axborotning konfedensialligi   
d) Ixchamligi

195. Foydalanishda boshqarishda ma’lumot , resurs, jarayon nima deb ataladi?

a) Obyekt   
b) Subyekt   
c) Tizim   
d) Ruxsat

196. Foydalanishni boshqarish –bu...

a) Subyektni Obyektga ishlash qobilyatini aniqlashdir.   
b) Subyektni Subyektga ishlash qobilyatini aniqlashdir.   
c) Obyektni mizojga ishlash qobilyatini aniqlashdir   
d) Autentifikatsiyalash jarayonidir

197. Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar qanday vazifani bajaradi?

a) Subyekt   
b) Obyekt   
c) Tizim   
d) Ruxsat

198. Foydalanishni boshqarishda subyekt bu - ....

a) Inson, dastur, jarayon   
b) Jarayon, dastur   
c) Ma’lumot, resurs, jarayon   
d) Resurs

199. Foydalanishni boshqarishning asosan nechta bor?

a) 4   
b) 5   
c) 6   
d) 7

200. Foydalanishni boshqarishning ….. usuli tizimdagi shaxsiy obyektlarni himoyalash uchun qo‘llaniladi?

a) Discretionary access control( DAC)   
b) Mandatory access control (MAC)   
c) Role-based access control (RBAC)   
d) Attribute based access control (ABAC)

201. Foydalanishni boshqarishning ….usulida foydalanishlar subyektlar va obyektlarni klassifikatsiyalashga asosan boshqariladi.

a) Mandatory access control (MAC)   
b) Discretionary access control( DAC)   
c) Role-based access control (RBAC)   
d) Attribute based access control (ABAC)

202. Foydalanishni boshqarishning …. usulida ruxsatlar va xarakatni kim bajarayotganligi to‘g‘risidagi xolatlar “agar, u xolda” buyrug‘idan tashkil topgan qoidalarga asoslanadi.

a) Attribute based access control (ABAC)   
b) Discretionary access control( DAC)   
c) Mandatory access control (MAC)   
d) Role-based access control (RBAC)

203. Foydalanishni boshqarishning …. usulida subyekt va obyektlarga tegishli huquqlarni ma’murlash oson kechadi.

a) Role-based access control (RBAC)   
b) Discretionary access control( DAC)   
c) Mandatory access control (MAC)   
d) Attribute based access control (ABAC)

204. Foydalanishni boshqarishning …. usulida xavfsizlik markazlashgan tarzda xavfsizlik siyosati ma’muri tomonidan amalga oshiriladi.

a) Mandatory access control (MAC)   
b) Discretionary access control( DAC)   
c) Role-based access control (RBAC)   
d) Attribute based access control (ABAC)

205. Foydalanishni boshqarishning Discretionary access control( DAC) usulidan asosan ….. qo‘llaniladi.

a) Operatsion tizimlarda   
b) Ma’lumotlar bazasida   
c) Web saytlarda   
d) Kompyuter tarmoqlarda

206. Tarmoqda foydalanuvchilarga tegishli ma’lumotlarini qo‘lga kiritub, uni hujum qiluvchiga yuboraradigan dasturiy kod qanday ataladi?

a) Spyware   
b) Rootkits   
c) Backdoors   
d) Ransomware

207. Kompyuter tarmoqdagi foydalanuvchilar harakatini, uning axborot resurslardan foydalanishga urinishini qayd etish qansi atama bilan nomlanadi?

a) Ma’murlash   
b) Identifikatsiyalash   
c) Autentifikatsiyalash   
d) Aniqlash

208. Global tamoq dastlab paytda qaysi nom bilan atalgan?

a) ARPANET   
b) NETWORK   
c) INTRANET   
d) INTERNET

209. ….-mavjud tahdidni amalga oshirilgan ko‘rinishi bo‘lib, bunda kutilgan tahdid amalga oshiriladi.

a) Hujum   
b) Tahdid   
c) Zaiflik   
d) Buzish

210. Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilarga tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni – bu…

a) Avtorizatsiya   
b) Identifikatsiya   
c) Autentifikatsiya   
d) Ma’murlash

211. IEEE 802.11, Wi-Fi standartini qo‘llovchi tarmoq turini aniqlang.

a) Lokal simsiz tarmoq   
b) Shaxsiy simsiz tarmoq   
c) Regional simsiz tarmoq   
d) Global simsiz tarmoq

212. IEEE 802.16, WiMAX standartini qo‘llovchi tarmoq turini aniqlang.

a) Shahar simsiz tarmoq   
b) Shaxsiy simsiz tarmoq   
c) Lokal simsiz tarmoq   
d) Global simsiz tarmoq

213. Elektron imzoni haqiqiyligini tekshirish … amalga oshiriladi.

a) Imzo muallifining ochiq kaliti yordamida   
b) Ma’lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida   
c) Ma’lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida   
d) Imzo muallifining maxfiy kaliti yordamida

214. DoS hujumlari oqibati quyidagilardan qaysi biri sodir bo‘ladi?

a) Foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan mahrum qilinadilar   
b) Foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzg‘unchilarga etkaziladi   
c) Axborot tizimidagi ma’lumotlar bazalari o‘g‘irlanib ko‘lga kiritilgach, ular yo‘q qilinadilar   
d) Foydalanuvchilar axborotlariga ruxsatsiz o‘zgartirishlar kiritilib, ularning yaxlitligi buziladi

215. Kriptografiga “Kalit” atamasiga qanday ta’rif beriladi?

a) axborotni shifrlash va deshifrlash uchun kerakli axborot   
b) Bir qancha kalitlar yig‘indisi   
c) Axborotli kalitlar to‘plami   
d) Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

216. Kalitlar boshqaruvi qanday elementga ega bo‘ladi?

a) hosil qilish, yig‘ish, taqsimlash   
b) ishonchliligi, maxfiyligi, aniqligi   
c) xavfsizlik, tez ishlashi, to‘g‘ri taqsimlanishi   
d) abonentlar soni, xavfsizligi, maxfiyligi

217. Kiberxavfsizkda “tahdid” atamasi qanday ta’riflanadi?

a) Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa   
b) Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa   
c) Bu riskni o‘zgartiradigan harakatlar   
d) Bu noaniqlikning maqsadlarga ta’siri

218. Kiberxavfsizlik nechta bilim soxasini o‘z ichiga oladi?

a) 8 ta   
b) 6 ta   
c) 5 ta   
d) 7 ta

219. Kiberxavfsizlikni ta’minlash masalalari bo‘yicha xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang.

a) SANS (System Administration Networking and Security)   
b) Department of defence (DOD)   
c) Discretionary access control   
d) Attribute based access control

220. Kimlar o‘zining harakatlari bilan sanoat josusi yetkazadigan muammoga teng (undan ham ko‘p bo‘lishi mumkin) muammoni yuzaga keltiradi?

a) Ishonchsiz xodimlar   
b) Xaker-proffesional   
c) Sarguzasht qidiruvchilar   
d) G‘oyaviy xakerlar

221. Kompyuter bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning xatti-harakatlari, komyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko‘rsatishini o‘rgatadigan soha nima deb ataladi?

a) Kiberetika   
b) Kiberhuquq   
c) Kiberqoida   
d) Kiberxavfsizlik

222. Tarmoq qurilmalari IPv4 manzilni to‘g‘ri kiritilishini ko‘rsating.

a) 172.25.100.100   
b) 12:AC:14:1C:3B:13   
c) 255.255.255.0   
d) 1001000110111

223. Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi…

a) Kompyuter tarmoqlari   
b) Kompyuter markazi   
c) Ma’lumotlar bazasi   
d) Tarmoq xavfsizligi

224. ….kompyuter tizimiga tahdid qilish imkoniyatiga ega va troyanlar, viruslar, “qurt”lar ko‘rinishida bo‘lishi mumkin.

a) Zararli dastur   
b) .exe fayl   
c) Boshqariluvchi dastur   
d) Kengaytmaga ega bo‘lgan fayl

225. ….bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida o‘zini ko‘rsatsada, yashiringan zararli koddan iborat.

a) troyan otlari   
b) adware   
c) spyware   
d) rootkits

226. ….zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi.

a) mantiqiy bombalar   
b) adware   
c) spyware   
d) rootkits

227. ….keng qamrovli nishondagi tizim va tarmoq resurlarida xizmatdan foydalanishni buzishga qaratilgan hujum bo‘lib, Internetdagi ko‘plab zombi kompyuterlar orqali bilvosita amalga oshiriladi.

a) Taqsimlangan DOS hujumlar   
b) O‘rtada turgan odam hujumi   
c) Parolga qaratilgan hujumlar   
d) Passiv razvedka hujumlari

228. Qaysi hujumlar asosan portlarni va operaesion tizimni skanerlashni maqsad qiladi?

a) Aktiv razvedka hujumlari   
b) O‘rtada turgan odam hujumi   
c) Parolga qaratilgan hujumlar   
d) Passiv razvedka hujumlari

229. …. hujumlari trafik orqali axborotni to‘plashga harakat qiladi. Buning uchun hujumchi sniffer deb nomlanuvchi dasturiy vositadan foydalanadi.

a) Passiv razvedka hujumlari   
b) Aktiv razvedka hujumlari   
c) O‘rtada turgan odam hujumi   
d) Parolga qaratilgan hujumlar

230. …. nishondagi kompyuter tizimi uchun nazoratni qo‘lga kiritish yoki ruxsatsiz foydalanish maqsadida amalga oshiriladi.

a) Passiv razvedka hujumlari   
b) Aktiv razvedka hujumlari   
c) O‘rtada turgan odam hujumi   
**d) Parolga qaratilgan hujumlar**

231. … hujumda hujum qiluvchi o‘rnatilgan aloqaga suqilib kiradi va aloqani uzadi.

a) Passiv razvedka hujumlari   
b) Aktiv razvedka hujumlari   
**c) O‘rtada turgan odam hujumi**   
d) Parolga qaratilgan hujumlar

232. Konfidentsial axborotdan foydalanish tushunchasi…

a) Muayyan shaxsga tarkibida konfidensial xarakterli ma’lumot bo‘lgan axborot bilan tanishishga vakolatli mansabdor shaxsning ruxsati.   
b) Korxona o‘z faoliyatini buzilishsiz va to‘xtalishsiz yurgiza oladigan vaqt bo‘yicha barqaror bashoratlanuvchi atrof-muhit holati.   
c) Ma’lumotlarning ma’lumotlar bazasiga tegishli darajasini aniqlash va belgilash.   
d) Olingan ma’lumotlar jo‘natuvchisining so‘ralganiga mosligini tasdiqlash

233. Kriptoanaliz qanday jarayonlarni o‘rganadi?

a) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi   
b) axborotni qayta akslantirishning texnik usullarini izlaydi va tadqiq qiladi   
c) axborotni akslantirib himoyalash muammosi bilan shug‘ullanadi   
d) kalitni qo‘llab matnni ochish imkoniyatlarini o‘rganadi

234. Kriptografiya qanday jarayonlarni o‘rganadi?

a) axborotni akslantirish va qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi   
b) axborotni qayta akslantirib himoyalash muammosi bilan shug‘ullanadi   
c) kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi   
d) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

235. Kriptologiya nechta yo‘nalishga bo‘linadi?

a) 2 ta   
b) 3 ta   
c) 4 ta   
d) 5 ta

236. Kompyuter tarmoqlarda qo‘llanuvchi topologiya turi qaysi?

a) Yulduz, shina, xalqa   
b) Markaziy, tengma-teng, aralash   
c) To‘liq bog‘langan, shina, aylana   
d) Shina, optik, koaksial

237. Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish jarayoni qanday ataladi?

a) Autentifikatsiya   
b) Identifikatsiya   
c) Ma’murlash (accaunting)   
d) Avtorizatsiya

238. Qog‘oz ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi?

a) 4 xil   
b) 8 xil   
c) 7 xil   
d) 5 xil

239. Ma’lumotlarni zaxira nusxalash bu – …

a) Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni   
b) Axborotni turli dasturlar yordamida tiklash imkoniyati   
c) Ma’lumotlarni ishonchli o‘chirish imkoniyati   
d) Ma'lumotlar xavfsizligini ta'minlash uchun qo‘llaniladigan shifrlash jarayoni

240. Turli offis ilovalari – MS Word hujjati, MS Excel elektron jadvali kabi fayllarni qaysi virus turi zararlaydi?

a) Makroviruslar   
b) Troyanlar   
c) Botnetlar   
d) Mutantvirus

241. Ma'lumotlarni zahira nusxasini saqlovchi va qayta tikovchi dasturni belgilang.

a) Redo Backup and Recovery   
b) BestCrypt   
c) Cryptool 1.4   
d) Eset32

242. Nomuntazam siyosat (Promiscuous Policy) nima?

a) Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi   
b) Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi   
c) Hamma narsa taqiqlanadi   
d) Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

243. OSI modelining birinchi sathi nomini belgilang.

a) Fizik sath (physical)   
b) Ilova sath (application)   
c) Seans sath (session)   
d) Kanal sath (data link)

244. OSI modelining ikkinchi sathi nomini belgilang .

a) Kanal sath (data link)   
b) Fizik sath (physical)   
c) Ilova sath (application)   
d) Seans sath (session)

245. OSI modelining uchinchi sathi nomini belgilang .

a) Tarmoq(network)   
b) Fizik sath (physical)   
c) Ilova sath (application)   
d) Seans sath (session)

246. OSI modelining to‘rtinchi sathi nomini belgilang .

a) Transport (transport)   
b) Fizik sath (physical)   
c) Ilova sath (application)   
d) Taqdimot (presentation)

247. OSI modelining beshinchi sathi nomini belgilang.

a) Seans sath (session)   
b) Fizik sath (physical)   
c) Ilova sath (application)   
d) Seans sath (session)

248. OSI modelining oltinchi sathi nomini belgilang.

a) Taqdimot (presentation)   
b) Fizik sath (physical)   
c) Ilova sath (application)   
d) Tarmoq(network)

249. OSI modelining yettinchi sathi nomini belgilang

a) Ilova sath (application)   
b) Seans sath (session)   
c) Fizik sath (physical)   
d) Tarmoq(network)

250. OSI modelida nechta sathdan iborat?

a) 7 ta   
b) 4 ta   
c) 5 ta   
d) 3 ta

251. OSI modelining Ilova sath (application) sathida qanday protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket   
b) ASCII, EBCDIC, JPEG, MIDI   
c) TCP, UDP, SCTP   
d) IPv4, IPv6, IPsec, AppleTalk, ICMP

252. OSI modelining Taqdimot (presentation) sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket   
**b) ASCII, EBCDIC, JPEG, MIDI**   
c) TCP, UDP, SCTP   
d) IPv4, IPv6, IPsec, AppleTalk, ICMP

253. OSI modelining Transport sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket   
b) ASCII, EBCDIC, JPEG, MIDI   
**c) TCP, UDP, SCTP**   
d) IPv4, IPv6, IPsec, AppleTalk, ICMP

254. OSI modelining Tarmoq (network) sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket   
b) ASCII, EBCDIC, JPEG, MIDI   
c) TCP, UDP, SCTP   
**d) IPv4, IPv6, IPsec, AppleTalk, ICMP**

255. OSI modelining Kanal (data link) sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket   
b) ASCII, EBCDIC, JPEG, MIDI   
c) TCP, UDP, SCTP   
**d) PPP, IEEE 802.22, Ethernet, DSL, ARP**

256. OSI modelining Fizik (physical) sathida qanday tarmoq qurilmalari qo‘llaniladi?

a) Marshrutizator   
b) Ko‘prik   
c) Tarmoq adapter   
**d) Kontsentrator**

257. OSI modelining Kanal (data link) sathida qanday tarmoq qurilmalar qo‘llaniladi?

a) Marshrutizator   
b) Ko‘prik   
c) Tarmoq ekrani   
**d) Kommutator**

258. OSI modelining Tarmoq (network) sathida qanday tarmoq qurilmalar qo‘llaniladi?

**a) Marshrutizator**   
b) Ko‘prik   
c) Tarmoq ekrani   
d) Kommutator

259. OSI modelining Fizik (physical) sathida axborot tipi qanday nomlanadi?

**a) bit**   
b) kadr   
c) paket   
d) segmet

260. OSI modelining Kanal (data link) sathida axborot tipi qanday nomlanadi?

a) ma’lumot   
**b) bit/kadr**   
c) paket   
d) segmet/datagramma

261. OSI modelining Tarmoq (network) sathida axborot tipi qanday nomlanadi?

a) ma’lumot   
b) bit/kadr   
**c) paket**   
d) segmet/datagramma

262. OSI modelining Transport sathida axborot tipi qanday nomlanadi?

a) ma’lumot   
b) bit/kadr   
c) paket   
**d) segmet/datagramma**

263. Paranoid siyosati (Paranoid Policy) – bu ….

**a) Hamma narsa ta’qiqlanadi**   
b) Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi   
c) Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi   
d) Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

264. Polimorf viruslar tushunchasi to‘g‘ri ko‘rsating.

a) Viruslar turli ko‘rinishdagi shifrlangan viruslar bo‘lib, o‘zining ikkilik shaklini nusxadan-nusxaga o‘zgartirib boradi   
b) Odatda foyl tarkibida yashirinib tarqaydi   
c) o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dasturkodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi   
d) Viruslar yuklangan qattiq diskdagi, disketa yoki fleshkasektorlarida joylashgan kichik programmalarni zararlaydi yoki uni almashtiradi.

265. Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi?

a) Shaxsiy tarmoq   
b) Lokal   
c) Mintaqaviy   
d) Campus

266. Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi?

a) DNS tizimlari   
b) TCP/IP   
c) Ethernet   
d) Token ring

267. Qanday hujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi?

a) Razvedka hujumlari   
b) Kirish hujumlari   
c) DOS hujumlari   
d) Zararli hujumlar

268. Qanday hujumda hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi?

a) Kirish hujumlari   
b) Razvedka hujumlari   
c) DOS hujumlar   
d) Zararli hujumlar

269. Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi?

a) Tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi   
b) Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi   
c) Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.   
d) Potensial zaiflikni aniqlash imkoniyati yo‘qligi

270. Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi?

a) Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi   
b) Tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi   
c) Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.   
d) Potensial zaiflikni aniqlash imkoniyati yo‘qligi

271. Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi?

a) Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.   
b) Tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi   
c) Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi   
d) Potensial zaiflikni aniqlash imkoniyati yo‘qligi

272. Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.

a) Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.   
b) Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.   
c) Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi   
d) Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi

273. Quyidagilardan MAN (metropolitan area network) tarmoqqa berilgan ta’rifni belgilang.

a) Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi   
b) Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.   
c) Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.   
d) Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi

274. Kompyuter tarmoqlaridan “Umumiy shina” topologiyasi xususiyati qanday?

a) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi   
b) Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi   
c) Yuboriluvchi va qabul qilinuvchi ma’lumot token yordamida manziliga yetkaziladi   
d) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi

275. Kompyuter tarmoqlaridan “Yulduzsimon” topologiyasiga ta'rif bering.

a) Har bir kompyuterni markaziy konsentrator bilan ulash orqali tashkil etiladi   
b) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi   
c) Yuboriluvchi va qabul qilinuvchi ma’lumot token yordamida manziliga yetkaziladi   
d) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi

276. Kompyuter tarmoqlaridan “Xalqasimon” topologiyasiga ta'rif bering.

a) Har bir kompyuter boshqa ikkita kompyuter bilan ulangan va signal aylana bo‘yicha o‘tadi   
b) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi   
c) Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi   
d) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi

277. Quyidagilardan qaysi birida tarmoqning “Uyali mesh” topologiyasiga ta'rif berilgan?

a) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi   
b) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi   
c) Yuboriluvchi va qabul qilinuvchi ma’lumot Token yordamida manziliga yetkaziladi   
d) Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi

278. Aksariyat tashkilotlar muhim ma’lumotlarini qaysi texnologiyasi asosida zaxira nusxalashni amalga oshiradilar?

a) Random Array of Independent Disks(RAID)   
b) Virtual private network(VPN)   
c) Point to Point   
d) HyperText Transfer Protocol(HTTP)

279. Ransomware zararli dasturi axborotlarga qanday zarar keltiradi?

a) mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi.   
b) marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.   
c) foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.   
d) bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi.

280. Ma ’murlash usuli bo‘yicha tarmoqlar qanday turlarga bo‘linadi?

a) “Bir rangli” va “mijoz server” turlarga   
b) Server va kliyent turlarga   
c) Asosiy va qo‘shimcha turlar   
d) Korporativ va xalqaro turlarga

281. Rezident bo‘lmagan viruslar qachon xotirani zararlaydi?

a) Faqat faollashgan vaqtida   
b) Faqat o‘chirilganda   
c) Kompyuter yoqilganda   
d) Tarmoq orqali ma’lumot almashishda

282. Risk, tahdid, zaiflik va ta’sir tushunchalari o‘rtasida o‘zaro bog‘lanish qanday ifodalanadi?

a) RISK = Tahdid x Zaiflik x Ta’sir   
b) RISK = Tahdid +Zaiflik + Ta’sir   
c) RISK = Tahdid x (Zaiflik +Ta’sir)   
d) RISK = Tahdid -Zaiflik +Ta’sir

283. Risk darajasi tarmoqga (yoki tizimga) natijaviy ta’sirning bahosi bo‘lib, quyidagi tenglik bilan ifodalanadi:

a) Risk darajasi = natija \* ehtimollik   
b) Risk darajasi = natija +ehtimollik.   
c) Risk darajasi = natija /ehtimollik.   
d) Risk darajasi = natija - ehtimollik.

284. Samarali risklarni boshqarishning rejasi risklarni aniqlashni va baholashni kafolatli amalga oshirishda …. va qayta ko‘rib chiqishni talab etadi.

a) Risk monitoringi   
b) Riskni tahlillash   
c) Muvaffaqiyatli risklar   
d) Tanazzulga uchragan risklar

285. Risk darajalari nechta turga bo‘linadi?

a) 4 ta   
b) 3 ta   
c) 2 ta   
**d) 5 ta**

286. Risklarni boshqarish –bu…

a) Risklarni aniqlash, baholash, javob berish va bo‘lishi mumkin bo‘lgan ta’sirga tashkilot tomonidan javob berilishini amalga oshirish jarayoni   
b) Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta’siri va ehtimolini o‘lchashni ta’minlaydi.   
c) Aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni.   
d) Risk monitoringi yangi risklarni paydo bo‘lish imkoniyatini aniqlash

287. Risklarni boshqarish jarayoni quyidagi asosiy nechta bosqichga ajratiladi?

a) 4 ta   
b) 2 ta   
c) 5 ta   
d) 3 ta

288. …. tashkilotning risklarni boshqarish usuliga amalga oshirish tadbirlarini belgilaydi va tashkilotda axborot xavfsizligi va risklarni boshqarish bo‘yicha faoliyatni birlashtimvchi tarkibiy jarayonni ta’minlaydi.

a) Risklarni boshqarish freymworki   
b) Risk monitoringi   
c) Riskni tahlillash   
d) Muvaffaqiyatli risklar

289. Rootkitlar qanday zararli amallar bajaradi?

a) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi   
b) bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi   
c) o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi   
d) ararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

290. Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?

a) Fizik nazorat   
b) Huquqiy nazorat   
c) Ma’muriy nazorat   
d) Tashkiliy nazorat

291. Shifrlash nima?

a) ochiq matnni shifrmatnga o‘zgartirish jarayoni   
b) shifrmatnni ochiq matnga o‘zgartiruvchi teskari jarayoni   
c) kalitni bilmasdan turib shifrmatn bo‘yicha ochiq matnni tiklash jarayoni   
d) alfavit elementlaridan tartiblangan nabor

292. Kriptotizim bu-…

a) ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o‘zgartirishlar oilasi   
b) shifrmatnni ochiq matnga o‘zgartiruvchi teskari jarayoni   
c) kalitni bilmasdan turib shifrmatn bo‘yicha ochiq matnni tiklash jarayoni   
d) alfavit elementlaridan tartiblangan nabor

293. Simmetrik kriptotizimlarda ... .

a) shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi   
b) bir-biriga matematik usullar bilan bog‘langan ochiq va yopiq kalitlardan foydalaniladi   
c) axborot ochiq kalit yordamida shifrlanadi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi   
d) kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi

294. Simsiz tarmoqlarni kategoriyalarini to‘g‘ri ko‘rsating?

a) Simsiz shaxsiy tarmoq, simsiz lokal tarmoq, simsiz shahar tarmoq va simsiz global tarmoq   
b) Simsiz internet tarmoq va Simsiz telefon tarmoq, Simsiz shaxsiy tarmoq va Simsiz global tarmoq   
c) Simsiz internet tarmoq va uy simsiz tarmog‘i   
d) Simsiz chegaralanmagan tarmoq , simsiz kirish nuqtalari

295. Spyware-qanday zararli dastur?

a) tarmoqda foydalanuvchilarga tegishli ma’lumotlarini qo‘lga kiritub, uni hujum qiluvchiga yuboraradigan dasturiy kod   
b) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.   
c) internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi   
d) zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi

296. Subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim qilish jarayoni nima?

a) Identifikatsiya   
b) Autentifikatsiya   
c) Avtorizatsiya   
d) Ma’murlash

297. Kompyuter virusining birinchi ta’rifni kim bergan?

a) 1984 yili Fred Koen   
b) 1951 yil Jon fon Neumann   
c) 1981 yil Elik Cloner   
d) 1990 yil Bill Geyts

298. Kompyuter viruslari hayot davrining ikkita asosiy bosqichini toping.

a) Saqlanish va bajarilish   
b) Yaralish va yashash   
c) Tarqalish va zararlash   
d) Zararlash va yo‘q bo‘lish

299. Kompyuter viruslarining bajarilish davri, odatda, nechta bosqichni o‘z ichiga oladi?

a) 5 ta   
b) 2 ta   
c) 3 ta   
d) 4 ta

300. O‘z-o‘zidan tarqalish mexanizmi amalga oshiriluvchi, tizimga zarar keltirmaydi, faqat diskdagi bo‘sh xotirani sarflaydigan viruslar qanday viruslar deb ataladi?

a) Beziyon viruslar   
b) Xavfsiz viruslar   
c) Xavfli viruslar   
d) Juda xavfli viruslar

301. Tizimda mavjudligi turli taassurot (ovoz, video) bilan bog‘liq, bo‘sh xotirani kamaytirsada, dastur va ma’lumotlarga ziyon yetkazmaydigan viruslar qanday viruslar deb ataladi?

a) Xavfsiz viruslar   
b) Beziyon viruslar   
c) Xavfli viruslar   
d) Juda xavfli viruslar

302. Kompyuter ishlashida jiddiy nuqsonlarga sabab bo‘luvchi, natijada dastur va ma’lumotlar buzilishiga olib kelivchi viruslar qanday viruslar deb ataladi?

a) Xavfli viruslar   
b) Xavfsiz viruslar   
c) Beziyon viruslar   
d) Juda xavfli viruslar

303. PPP-kadrlarni tarmoq sathi paketlariga inkapsulyatsiyalovchi kanal sathining tunnel protokolini belgilang.

a) L2TP (Layer 2 Tunneling Protocol)   
b) IPSec (IP Security)   
c) PPTP (Point-to-Point Tunneling Protocol)   
d) SSH (Secure Shell)

304. “nuqta-nuqta” xilidagi kanal sathining tunnel protokolini belgilang.

a) IPSec (IP Security)   
b) PPTP (Point-to-Point Tunneling Protocol)   
c) SSH (Secure Shell)   
d) L2TP (Layer 2 Tunneling Protocol)

305. Tarmoqlararo ekran (firewall, brandmaver) –bu…

a) Trafikni filtrlash mexanizmiga asoslangan tarmoqdan foydalanishni cheklashning bazaviy vositasi   
b) Qurilma perimetrli himoyalash masalasining kompleks yechimi hisoblanadi   
c) Ma’lumotlarni inkapsulyatsiyalash mexanizmlari, hamda qo‘shimcha autentifikatsiya, shifrlash, yaxlitlikni nazoratlash

306. Kiruvchi ma’lumotning uzunligi o‘zgaruvchan, chiqishda esa o‘zgarmas uzunlikdagi qiymatni qaytaradigan jarayon qanday ataladi?

a) Xesh funksiya   
b) О‘rniga qoyish akslantirish   
c) O‘rin almashtirish akslantirishi   
d) Elektron raqamli imzo

307. Ochiq matn simvollari bir alfavitdan olinib, unga mos shifrmatn simvollari boshqa bir alfavitdan olinadigan jarayon nomini belgilang.

a) О‘rniga qoyish akslantirish   
b) Xesh funksiya   
c) O‘rin almashtirish akslantirishi   
d) Elektron raqamli imzo

308. Ochiq matnda ishtirok etgan simvollar shifrmatnda ham ishtirok etib, faqat ularning o‘rnii almashadigan jarayon nomini belgilang.

a) O‘rin almashtirish akslantirishi   
b) О‘rniga qoyish akslantirish   
c) Xesh funksiya   
d) Elektron raqamli imzo

309. …. ashkilotning va u bilan bog‘liq boshqa komponentlar va interfeyslarning istalgan axborot xavfsizligi tizimi xolatini tavsiflaydi.

a) Kiberxavfsizlik arxitekturasi   
b) Kiberxavfsizlik siyosati   
c) Simmetrik shiflash   
d) Elektron raqamli imzo

310. Fishing hujumi usullari to‘g‘ri ko‘rsatilgan qatorni belgilang: 1.Soxta havola; 2.soxta lotereya; 3.TV reklama; 4. Tekin dasturlar; 5.DOS hujum 6.Razvedka

a) 1,2,4   
b) 2,3,5   
c) 3,5,6   
d) 4,5,6

Xato   
Qaysi siyosat tizim resurslarini foydalanishda hech qanday cheklovlar qo‘ymaydi?

Paranoid siyosat   
Zаxirаlаshning qаndаy turlаri mаvjud?   
Ichki, tаshqi   
Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ... .   
Hakker   
Axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi nima deb ataladi?   
Axborot tizimlari   
Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?   
RAID 0   
Spam bilan kurashishning dasturiy uslubida nimalar ko‘zda tutiladi?   
Elektron pochta qutisiga kelib tushadigan spamlar me’yoriy xujjatlar asosida cheklanadi va bloklanadi   
Botnet-nima?   
zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish.   
Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi?   
RAID 5   
Zararli dasturlar qanday turlarga bo‘linadi?   
Tabiiy dasturlar va suniy dasturlar   
Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o‘z ichiga oladi?   
Davlat va nodavlat tashkilotlari me’yorlarni   
Ma’lumotlarni zaxira nusxalash bu – …   
Ma'lumotlar xavfsizligini ta'minlash uchun qo‘llaniladigan shifrlash jarayoni   
Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...   
Global tarmoqdan uzib qo‘yish   
Dаstlаbki virus nechаnchi yildа yarаtilgаn?   
1988   
System-Specific SecurityPolicies, SSSP-bu…   
Muammoga qaratilgan xavfsizlik siyosati   
Enterprise Information Security Policies, EISP-bu…   
Tizimga qaratilgan xavfizlik siyosati   
Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?   
"To‘liq zaxiralash"   
"To‘q sariq kitob"da xavfsizlik kriteriyalari qanday bo‘limlardan iborat?   
O‘ta maxfiy, maxfiy

TO’G’RILARI:

OSI modelida nechta tarmoq satxi bor ?   
J: 7   
OSI modelining birinchi satxi qanday nomlanadi   
J: Fizik satx   
OSI modelining ikkinchi satxi qanday nomlanadi   
J: Kanal satxi   
OSI modelining uchinchi satxi qanday nomlanadi   
J: Tarmoq satxi   
OSI modelining oltinchi satxi qanday nomlanadi   
J: Taqdimlash satxi   
OSI modelining yettinchi satxi qanday nomlanadi   
J: Amaliy satx   
OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi   
J: fizik, kanal va tarmoq satxlari   
OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi   
J: Marshrutizator   
OSI modelining fizik satxi qanday funktsiyalarni bajaradi   
J: Elektr signallarini uzatish va qabul qilish   
Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ?   
J: Obyekt    
Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?   
J: Subyekt   
Simmetrik kriptotizimlarda ... jumlani davom ettiring   
J: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi   
Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.   
J: 2 turga   
Axborotning eng kichik o’lchov birligi nima?   
J: bit   
Ko‘z pardasi, yuz tuzilishi, ovoz tembri-: bular autentifikatsiyaning qaysi faktoriga mos belgilar?   
J: Biometrik autentifikatsiya   
Kriptografiyaning asosiy maqsadi...   
J: maxfiylik, yaxlitlilikni ta`minlash   
Ro’yxatdan o’tish bu?   
foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni   
Qanday xujumda zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi?   
J: Zararli hujumlar   
Qanday xujumda hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi?   
J: Kirish hujumlari   
Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub   
J: Ethernet, FDDI   
Xesh-:funktsiyani natijasi …   
J: fiksirlangan uzunlikdagi xabar   
Ethernet kontsentratori qanday vazifani bajaradi   
J: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi   
Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?   
J: fleshka, CD va DVD disklar   
Faol hujum turi deb…   
J: Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon   
Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi.   
J: MAC   
Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo‘llaniladi   
J: DAC   
Foydalanishni boshqarishning qaysi modelida Obyekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi   
J: DACfInternetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?   
Foydalanishni boshqarishning qaysi usuli -: Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.   
J: ABAC   
Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun Obyektlardan foydalanish ruxsati ko‘rsatiladi?   
J: RBAC   
To’rtta bir-:biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub   
J: Xalqa Yulduz To’liq bog’lanishli Yacheykali   
Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi?   
J: DNS tizimlari, Razvedka hujumlari   
…… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.   
J: Kiberxavfsizlik   
Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?   
J: raqamli imzoni shakllantirish va tekshirish muolajasi   
Kriptologiya -:   
J: axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi   
Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?   
J: Deshifrlash   
Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.   
J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik   
Autentifikatsiya faktorlari nechta   
J: 3   
Kriptografiyada matn –   
J: alifbo elementlarining tartiblangan to’plami   
Konfidentsiallikga to’g’ri ta`rif keltiring.   
J: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;   
Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-:ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu?   
J: login   
Kriptoanaliz –   
J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi   
sifatlarga ega bo’lishi kerak?   
J: ishonchli, qimmatli va to’liq   
Shifrlash –   
J: akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi   
Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?   
J: simmetrik kriptosistemalar   
Foydalanishni boshqarish –bu...   
J: Subyektni Obyektga ishlash qobilyatini aniqlashdir.   
Kompyuterning tashqi interfeysi deganda nima tushuniladi?   
J: kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari   
Kodlash nima?   
J: Ma’lumotni osongina qaytarish uchun hammaga   
Tarmoq kartasi bu...   
J: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.   
Elektron raqamli imzo deb –   
J: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha   
Hab bu...   
J: ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.   
Switch bu...   
J: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.   
Axborot xavfsizligining asosiy maqsadlaridan biri-: bu…   
J: Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish   
Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-:ketligi (maxfiy so’z) – bu?   
J: parol   
Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?   
J: SMTP, POP yoki IMAR   
Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi?   
J: Tez, aniq va maxfiyligiga   
Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.   
J: Yozish   
Qanday xujumda hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi?   
J: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari   
Kalit – bu …   
J: Matnni shifrlash va shifrini ochish uchun kerakli axborot   
Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi   
J: Fizik satx   
Blokli shifrlash-:   
J: shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish   
Kriptobardoshlilik deb …   
J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi   
Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi   
J: Xesh funksiyalar   
Kriptografiya –   
J: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi   
Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub   
J: TCP,UDP   
Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu -:   
J: steganografiya   
Yaxlitlikni buzilishi bu -: …   
J: Soxtalashtirish va o’zgartirish   
Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?   
J: barchasi   
Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub   
J: Ethernet, FDDI   
Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?   
J: Foydalanishni boshqarish   
Tarmoq repiteri bu…   
J: Signalni tiklash yoki qaytarish uchun foydalaniladi.   
Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?   
J: Ochiq kalitli kriptotizimlarda bir-:biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi   
Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi   
J: O‘qish   
MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi   
J: xavfsizlik siyosati ma’muri   
Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?   
J: Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi   
Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi   
J: Tarmoq satxi   
Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bog‘liq..   
J: Tashkilotda Obyektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi   
Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi   
J: {d, n} – yopiq, {e, n} – ochiq;   
Diskni shifrlash nima uchun amalga oshiriladi?   
J: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi   
Tahdid nima?   
J: Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.   
Risk   
J: Potensial foyda yoki zarar   
barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi?   
J: Fizik satx   
Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...   
J: Avtorizatsiya   
Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.   
J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik   
Kompyuter tarmoqlari bu –   
J: Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan   
Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?   
J: raqamli imzoni shakllantirish va tekshirish muolajasi   
Kriptografiyada matn –   
J: alifbo elementlarining tartiblangan to’plami   
Autentifikatsiya jarayoni qanday jarayon?   
J: obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash   
Rol tushunchasiga ta’rif bering.   
J: Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin   
Avtorizatsiya jarayoni qanday jarayon?   
J: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni   
Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima   
J: Parol   
Elektron raqamli imzo deb –   
J: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha   
TCP/IP modelida nechta satx mavjud   
J: 4   
Kriptoanaliz –   
J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi   
Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi?   
J: Simmetrik va assimetrik   
Shifrlash nima?   
J: Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi   
Kriptografiyada alifbo –   
J: axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam   
Kripto tizimga qo’yiladigan umumiy talablardan biri   
J: shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak   
Simmetrik kriptotizmning uzluksiz tizimida …   
J: ochiq matnning har bir harfi va simvoli alohida shifrlanadi   
Axborot resursi – bu?   
J: axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi   
Stenografiya ma’nosi...   
J: sirli yozuv   
Identifikatsiya jarayoni qanday jarayon?   
J: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni   
Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.   
J: Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.   
2. Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq?   
J:simmetrik kriptotizimlar   
3. Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.   
J:Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.   
4. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?   
J: parol   
5. Rol tushunchasiga ta’rif bering.   
Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin   
6. Foydalanish huquqini cheklovchi matritsa modeli bu...   
J:Bella La-Padulla modeli   
8. Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?   
J: Deshifrlash   
9. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?   
J:Strukturalarni ruxsatsiz modifikatsiyalash   
10. Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi?   
J:Kriptobardoshlik   
11. Foydalanishni boshqarish –bu...   
J: Sub’ektni Ob’ektga ishlash qobilyatini aniqlashdir.   
12. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?   
J: Yulduz   
13. RSA algoritm qaysi yilda ishlab chiqilgan?   
J: 1977 yil   
14. Elektron xujjatlarni yo‘q qilish usullari qaysilar?   
J:Shredirlash, magnitsizlantirish, yanchish   
15. Kriptografiyada kalitning vazifasi nima?   
J: Matnni shifrlash va shifrini ochish uchun kerakli axborot   
16. WiMAX qanday simsiz tarmoq turiga kiradi?   
J: Regional   
17. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…   
J: login   
18. Stenografiya ma’nosi qanday?   
J: sirli yozuv   
19. Fire Wall ning vazifasi...   
J: Tarmoqlar orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta’minlaydi   
20. Yaxlitlikni buzilishi bu - …   
J: Soxtalashtirish va o‘zgartirish

1. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko‘rsating?

DDoS (Distributed Denial of Service) hujum

1. Rezident virus…

tezkor xotirada saqlanadi

1. Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyoti fanda qanday nomladi?

AKT xavfsizlik siyosati

1. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.

Recuva, R.saver

1. Zaiflik – bu…

tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

1. Axborot xavfsizligi timsollarini ko‘rsating.

Alisa, Bob, Eva

1. Kiberetika tushunchasi:

Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

1. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuni qachon kuchga kirgan?

1997 yil 24 aprel

1. DIR viruslari nimani zararlaydi?

FAT tarkibini zararlaydi

1. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

Detektorlar

1. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?

"Issiq zaxiralash"

1. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...

Tamoqlararo ekranlarning o‘rnatilishi

1. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan

1. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…

Kiberjinoyat deb ataladi

1. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud?

detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar

1. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?

Ruxsat berishga asoslangan siyosat

1. DIR viruslari nimani zararlaydi?

FAT tarkibini zararlaydi

1. Makroviruslar nimalarni zararlaydi?

Ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.

1. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.

HandyBakcup

1. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.

"Sovuq saxiralash"

1. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.

Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

1. Polimorf viruslar tushunchasi to‘g‘ri ko‘rsating.

Viruslar turli ko‘rinishdagi shifrlangan viruslar bo‘lib, o‘zining ikkilik shaklini nusxadan-nusxaga o‘zgartirib boradi

1. Fishing (ing. Phishing – baliq ovlash) bu…

Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

|  |  |  |
| --- | --- | --- |
|  | Xavfsizlikning asosiy yo’nalishlarini sanab o’ting. | Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik |
|  | Axborot xavfsizligining asosiy maqsadlaridan biri- bu… | Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish |
|  | Konfidentsiallikga to’g’ri ta`rif keltiring. | axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; |
|  | Yaxlitlikni buzilishi bu - … | Soxtalashtirish va o’zgartirish |
|  | ... axborotni himoyalash tizimi deyiladi. | Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi |
|  | Kompyuter virusi nima? | maxsus yozilgan va zararli dastur |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya mahnosi... | sirli yozuv |
|  | Kriptologiya yo’nalishlari nechta? | 2 |
|  | Kriptografiyaning asosiy maqsadi... | maxfiylik, yaxlitlilikni ta`minlash |
|  | SMTP - Simple Mail Transfer protokol nima? | elektron pochta protokoli |
|  | SKIP protokoli... | Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi |
|  | Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar… | uzilish, tutib qolish, o’zgartirish, soxtalashtirish |
|  | ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. | konfidentsiallik |
|  | Foydalanish huquqini cheklovchi matritsa modeli bu... | Bella La-Padulla modeli |
|  | Kommunikatsion qism tizimlarida xavfsizlikni ta`minlanishida necha xil shifrlash ishlatiladi? | 2 |
|  | Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? | TCP/IP, X.25 protokollar |
|  | Himoya tizimi kompleksligiga nimalar orqali erishiladi? | Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali |
|  | Kalit – bu … | Matnni shifrlash va shifrini ochish uchun kerakli axborot |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | simmetrik kriptotizimlar |
|  | Autentifikatsiya nima? | Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi |
|  | Identifikatsiya bu- … | Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni |
|  | O’rin almashtirish shifri bu - … | Murakkab bo’lmagan kriptografik akslantirish |
|  | Simmetrik kalitli shifrlash tizimi necha turga bo’linadi. | 2 turga |
|  | Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular … | hosil qilish, yig’ish, taqsimlash |
|  | Kriptologiya - | axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi |
|  | Kriptografiyada alifbo – | axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam |
|  | Simmetrik kriptotizimlarda ... jumlani davom ettiring | shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi |
|  | Kriptobardoshlilik deb … | kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Elektron raqamli imzo deb – | xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha |
|  | Kriptografiya – | axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi |
|  | Kriptografiyada matn – | alifbo elementlarining tartiblangan to’plami |
|  | Kriptoanaliz – | kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Shifrlash – | akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi |
|  | Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi? | Tez, aniq va maxfiyligiga |
|  | Faol hujum turi deb… | Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon |
|  | Blokli shifrlash- | shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish |
|  | Simmetrik kriptotizmning uzluksiz tizimida … | ochiq matnning har bir harfi va simvoli alohida shifrlanadi |
|  | Kripto tizimga qo’yiladigan umumiy talablardan biri | shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak |
|  | Quyidagi tengliklardan qaysilari shifrlash va deshifrlashni ifodalaydi? | Ek1(T)=T, Dk2(T1)=T |
|  | Berilgan ta`riflardan qaysi biri assimmetrik tizimlarga xos? | Assimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi |
|  | Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang | Vijiner matritsasi, Sezar usuli |
|  | Akslantirish tushunchasi deb nimaga aytiladi? | 1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga |
|  | Simmetrik guruh deb nimaga aytiladi? | O’rin almashtirish va joylashtirish |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | simmetrik kriptositemalar |
|  | Xavfli viruslar bu - … | kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Elektron raqamli imzo tizimi qanday muolajani amalga oshiradi? | raqamli imzoni shakllantirish va tekshirish muolajasi |
|  | Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? | Simmetrik va assimetrik |
|  | Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin? | Korporativ va umumfoydalanuvchi |
|  | Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo’linadi? | Sust va faol |
|  | Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? | SMTP, POP yoki IMAR |
|  | Axborot resursi – bu? | axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi |
|  | Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu? | login |
|  | Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu? | parol |
|  | Identifikatsiya jarayoni qanday jarayon? | axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni |
|  | Autentifikatsiya jarayoni qanday jarayon? | ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash |
|  | Avtorizatsiya jarayoni qanday jarayon? | foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni |
|  | Ro’yxatdan o’tish bu? | foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni |
|  | Axborot qanday sifatlarga ega bo’lishi kerak? | ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | bit |
|  | Elektronhujjatning rekvizitlari nechta qismdan iborat? | 4 |
|  | Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? | fleshka, CD va DVD disklar |
|  | Imzo bu nima ? | hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati. |
|  | Muhr bu nima? | hujjatning haqi-qiyligini va biror bir yuridik shaxsga tegishli ekanligi-ni tasdiqlovchi isbotdir. |
|  | DSA – nima | Raqamli imzo algoritmi |
|  | El Gamal algoritmi qanday algoritm | Shifrlash algoritmi va raqamli imzo algoritmi |
|  | Sezarning shifrlash sistemasining kamchiligi | Harflarning so’zlarda kelish chastotasini yashirmaydi |
|  | Axborot xavfsizligi va xavfsizlik san’ati haqidagi fan …. deyiladi? | Kriptografiya |
|  | Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu - | steganografiya |
|  | Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? | Deshifrlash |
|  | …… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. | Kiberxavfsizlik |
|  | Risk | Potensial foyda yoki zarar |
|  | Kiberxavfsizlik nechta bilim soxasini o‘z ichiga oladi. | 8 |
|  | “Ma’lumotlar xavfsizligi” bilim sohasi...... | ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi. |
|  | “Dasturiy ta’minotlar xavfsizligi” bilim sohasi..... | foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi. |
|  | “Tashkil etuvchilar xavfsizligi” ..... | katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi. |
|  | “Aloqa xavfsizligi” bilim sohasi...... | tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi. |
|  | “Tizim xavfsizligi” bilim sohasi…… | tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi. |
|  | “Inson xavfsizligi” bilim sohasi…. | kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi. |
|  | “Tashkilot xavfsizligi” bilim sohasi …. | tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini |
|  | “Jamoat xavfsizligi” bilim sohasi ….. | u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi. |
|  | Tahdid nima? tizim yoki | Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
|  | Kodlash nima? | Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir |
|  | Shifrlash nima? | Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi |
|  | Bir martalik bloknotda Qanday kalitlardan foydalaniladi? | Ochiq kalitdan |
|  | Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing. | 23 |
|  | Agar RSA algotirmida n ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi. | M = Cd mod n; |
|  | O’nlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq tizi miga o’tkazing. 65 | 100001 |
|  | Quyidagi modulli ifodani qiymatini toping. (125\*45)mod10. | 5 |
|  | Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256. | 244 |
|  | Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi. | C = Me mod n; -tog’ri javob |
|  | Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi | Kriptologiya. |
|  | Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi | {*d, n*} – yopiq, {*e, n*} – ochiq; |
|  | Zamonaviy kriptografiya qanday bo’limlardan iborat? | Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish |
|  | 1. Kriptografik usullardan foydalanishning asosiy yo’nalishlari nimalardan iborat? | Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarni haqiqiyligini aniqlash, tashuvchilarda axborotlarni shifrlangan ko’rinishda saqlash (masalan, hujjatlarni, ma’lumotlar bazasini) |
|  | Shifr nima? | Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm |
|  | Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? | Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi |
|  | Oqimli shifrlashning mohiyati nimada? | Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur, Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi |
|  | Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating. | uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim, |
|  | Kriptotizim quyidagi komponentlardan iborat: | ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, Ek : M ® C (shifrlash uchun) va Dk: C®M (deshifrlash uchun) funktsiyalar |
|  | Serpent, Square, Twofish, RC6 , AES algoritmlari qaysi turiga mansub? | simmetrik blokli algoritmlar |
|  | DES algoritmiga muqobil bo’lgan algoritmni ko’rsating. | Uch karrali DES, IDEA, Rijndael |
|  | DES algoritmining asosiy muammosi nimada? | kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas |
|  | Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? | shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun |
|  | 12+22 mod 32 ? | 2 |
|  | 2+5 mod32 ? | 7 |
|  | Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi. | ochiq kalitlar |
|  | 12+11 mod 16 ? | 7 |
|  | RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo’llab quvvatlaydi. | 128 bitli, 192 bitli, 256 bitli |
|  | Xesh-funktsiyani natijasi … | uzunlikdagi xabar |
|  | RSA algoritmi qanday jarayonlardan tashkil topgan | Kalitni generatsiyalash; Shifrlash; Deshifrlash. |
|  | RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida necha bit bo‘lishi talab etiladi. | 2048 |
|  | Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi | Xesh funksiyalar |
|  | To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub | Xalqa |
|  | Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo’llamasligi mumkin | to’liq bog’lanishli |
|  | Kompyuterning tashqi interfeysi deganda nima tushuniladi | kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari |
|  | Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi | Yulduz |
|  | Ethernet kontsentratori qanday vazifani bajaradi | kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi |
|  | OSI modelida nechta sath mavjud | 7 |
|  | OSI modelining to’rtinchi sathi qanday nomlanadi | Transport sathi |
|  | OSI modelining beshinchi sathi qanday nomlanadi | Seanslar sathi |
|  | OSI modelining birinchi sathi qanday nomlanadi | Fizik sath |
|  | OSI modelining ikkinchi sathi qanday nomlanadi | Kanal sathi |
|  | OSI modelining uchinchi sathi qanday nomlanadi | Tarmoq sathi |
|  | OSI modelining oltinchi sathi qanday nomlanadi | Taqdimlash sathi |
|  | OSI modelining ettinchi sathi qanday nomlanadi | Amaliy sath |
|  | OSI modelining qaysi sathlari tarmoqqa bog’liq sathlar hisoblanadi | fizik, kanal va tarmoq sathlari |
|  | OSI modelining tarmoq sathi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi | Marshrutizator |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi | Fizik sath |
|  | Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi sathi bajaradi | Tarmoq sathi |
|  | Keltirilgan protokollarning qaysilari tarmoq sathi protokollariga mansub | IP, IPX |
|  | Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub | TCP,UDP |
|  | OSI modelining fizik sathi qanday funktsiyalarni bajaradi | Elektr signallarini uzatish va qabul qilish |
|  | OSI modeliningamaliy sathi qanday funktsiyalarni bajaradi | Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | Keltirilgan protokollarning qaysilari kanal sathi protokollariga mansub | Ethernet, FDDI |
|  | Keltirilgan protokollarning qaysilari taqdimlash sathi protokollariga mansub | SNMP, Telnet |
|  | Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu... | Avtorizatsiya |
|  | Autentifikatsiya faktorlari nechta | 3 |
|  | Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima | Parol |
|  | Ko‘z pardasi, yuz tuzilishi, ovoz tembri. | Biometrik autentifikatsiya |
|  | barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi. | Fizik satx |
|  | Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi | 2 |
|  | Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi. | Foydalanishni boshqarish |
|  | Foydalanishni boshqarish –bu... | sub’ektni sub’ektga ishlash qobilyatini aniqlashdir. |
|  | Foydalanishna boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi, | Sub’ekt |
|  | Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ? | Ob’ekt |
|  | Foydalanishna boshqarishning nechta usuli mavjud? | 4 |
|  | Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy ob’ektlarni himoyalash uchun qo‘llaniladi | DAC |
|  | Foydalanishni boshqarishning qaysi modelida ob’ekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi | DAC |
|  | Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi. | MAC |
|  | Foydalanishni boshqarishning mandatli modelida Ob’ektning xavfsizlik darajasi nimaga bog‘liq.. | Tashkilotda ob’ektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi |
|  | MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi | xavfsizlik siyosati ma’muri |
|  | Agar sub’ektning xavfsizlik darajasida ob’ektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi | O‘qish |
|  | Agar sub’ektning xavfsizlik darajasi ob’ektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi. | Yozish |
|  | Foydalanishni boshqarishning qaysi modelida har bir ob’ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun ob’ektlardan foydalanish ruxsati ko‘rsatiladi? | RBAC |
|  | Rol tushunchasiga ta’rif bering. | Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin |
|  | Foydalanishni boshqarishning qaysi usuli - ob’ektlar va sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. | ABAC |
|  | XACML foydalanishni boshqarishni qaysi usulining standarti? | ABAC |
|  | Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan? | barchasi |
|  | Axborotning kriptografik himoya vositalari necha turda? | 3 |
|  | Dasturiy shifrlash vositalari necha turga bo‘linadi | 4 |
|  | Diskni shifrlash nima uchun amalga oshiriladi? | Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi |
|  | Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi? | 4 |
|  | Kompyuter tarmoqlari bu – | Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi |
|  | Tarmoq modeli –bu.. ikki | Hisoblash tizimlariorasidagi aloqani ularning ichki tuzilmaviy vatexnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir to‘plami |
|  | OSI modelida nechta tarmoq sathi bor | 7 |
|  | OSI modeli 7 stahi bu | Ilova |
|  | OSI modeli 1 stahi bu | Fizik |
|  | OSI modeli 2 stahi bu | Kanal |
|  | TCP/IP modelida nechta satx mavjud | 4 |
|  | Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi. | Shaxsiy tarmoq |
|  | Tarmoq kartasi bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Switch bu... | Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi |
|  | Hab bu... | ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. |
|  | Tarmoq repiteri bu... | Signalni tiklash yoki qaytarish uchun foydalaniladi. |
|  | Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi. | DNS tizimlari |
|  | ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. | TCP |
|  | …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi. | UDP |
|  | Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi. | IP |
|  | Tarmoq taxdidlari necha turga bo‘linadi | 4 |
|  | Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; | Razvedka hujumlari |
|  | Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi | Kirish hujumlari |
|  | Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi; | Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari |
|  | Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi; | Zararli hujumlar |
|  | Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? | Imzo qo‘yish va imzoni tekshirishdan |
|  | Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? | Imzo muallifining ochiq *kaliti yordamida* |
|  | Tarmoq modeli-bu... | Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir |
|  | OSI modeli nechta sathga ajraladi? | 7 |
|  | Fizik sathning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | Ilova sathning vazifasi nimadan iborat | Ilovalarni tarmoqqa ulanish jarayoni |
|  | Kanal sathning vazifasi nimadan iborat | Fizik manzillash |
|  | Tarmoq sathning vazifasi nimadan iborat | Yo‘lni aniqlash va mantiqiy manzillash |
|  | TCP/IP modeli nechta sathdan iborat | 4 |
|  | Quyidagilarninf qaysi biri Kanal sathi protokollari | Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri tarmoq sathi protokollari | . IP, ICMP, ARP, RARP |
|  | Quyidagilarninf qaysi biri transport sathi protokollari | TCP, UDP, RTP |
|  | Quyidagilarninf qaysi biri ilova sathi protokollari | HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP va hak |
|  | TCP/IP modelining kanal sathiga OSI modelining qaysi sathlari mos keladi | Kanal, Fizik |
|  | TCP/IP modelining tarmoq sathiga OSI modelining qaysi sathlari mos keladi | Tarmoq |
|  | TCP/IP modelining transport sathiga OSI modelining qaysi sathlari mos keladi | Tramsport |
|  | TCP/IP modelining ilova sathiga OSI modelining qaysi sathlari mos keladi | Ilova, taqdimot, seans |
|  | Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang. | . Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi. |
|  | Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang. | Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi |
|  | Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang. | Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi |
|  | Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan | Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi |
|  | Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan | Yuboriluvchi va qabul qilinuvchi ma’lumot TOKYeN yordamida manziliga yetkaziladi |
|  | Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan | Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi |
|  | Tarmoq kartasi nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Repetir nima? | Odatda signalni tiklash yoki qaytarish uchun foydalaniladi |
|  | Hub nima? | Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi |
|  | Switch nima? | Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi |
|  | Router nima? | Qabul qilingan ma’lumotlarni tarmoq sathiga tegishli manzillarga ko‘ra (IP manzil) uzatadi |
|  | DNS tizimlari. | Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi |
|  | TCP bu- … | Transmission Control Protocol |
|  | UDP bu-… | User datagram protocol |
|  | Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang | Ichki, tashqi |
|  | Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi | Biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi | Hujum natijasida ishlab chiqarishi yo‘qolgan hollarda uni qayta tiklash ko‘p vaqt talab qiladi va bu vaqtda ishlab chiqarish to‘xtab qoladi |
|  | Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi | Konfidensial axborotni chiqib ketishi natijasida, tashkilot shaxsiy ma’lumotlarini yo‘qolishi mumkin |
|  | Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi | Tashkilot xodimlarining shaxsiy va ishga oid ma’ulmotlarini kutilmaganda oshkor bo‘lishi ushbu xodimlarga bevosita ta’sir qiladi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi | tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. | Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi. |
|  | Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi | Razvedka hujumlari |
|  | Ma’lumotlarni zaxira nusxalash bu – … | Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi |
|  | Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz | Zaxira nusxalash |
|  | Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi? | 5 |
|  | Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. | 4 |
|  | Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | RAID texnologiyasining transkripsiyasi qanday. | Random Array of Independent Disks |
|  | RAID texnologiyasida nechta satx mavjud | 6 |
|  | OSI modelining birinchi sathi qanday nomlanadi | Fizik sath |
|  | OSI modelining ikkinchi sathi qanday nomlanadi | Kanal sathi |
|  | OSI modelining uchinchi sathi qanday nomlanadi | Tarmoq sathi |
|  | OSI modelining oltinchi sathi qanday nomlanadi | Taqdimlash sathi |
|  | OSI modelining ettinchi sathi qanday nomlanadi | Amaliy sath |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi | Fizik sath |
|  | Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub | TCP,UDP |
|  | OSI modelining fizik sathi qanday funktsiyalarni bajaradi | Elektr signallarini uzatish va qabul qilish |
|  | OSI modelining amaliy sathi qanday funktsiyalarni bajaradi | Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | 12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan sonlar soni nechta? | 8 ta |
|  | Yevklid algoritmi qanday natijani beradi? | Sonning eng katta umumiy bo’luvchisini toppish |
|  | Qanday sonlar tub sonlar deb yuritiladi? | Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi. |
|  | To‘liq zaxiralash | To‘liq va o‘sib boruvchi usullarning mujassamlashgan ko‘rinishi bo‘lib, oxirgi zaxiralangan nusxadan boshlab bo‘lgan o‘zgarishlarni zaxira nusxalab boradi. • Amalga oshirish to‘liq zaxiralashga qaraganda tez amalga oshiriladi. • Qayta tiklash o‘sib boruvchi zaxiralashga qaraganda tez amalga oshiriladi. • Ma’lumotni saqlash uchun to‘liq zaxiralashga qaraganda kam joy talab etadi |
|  | O‘sib boruvchi zaxiralash | Zaxiralangan ma’lumotga nisbatan o‘zgarish yuz berganda zaxirilash amalga oshiriladi. • Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usuli bo‘lishi mumkin (to‘liq saxiralashdan). • Saqlash uchun kam hajm va amalga oshirish jarayoni tez |
|  | Differensial zaxiralash | Ushbu zaxiralashda tarmoqga bog‘lanishamalga oshiriladi. • Iliq zaxiralashda, tizim yangilanishi davomiy yangilanishni qabul qilish uchun ulanadi |
|  | Ushbu jarayon ma’lumot qanday yo‘qolgani, ma’lumotni qayta tiklash dasturiy vositasi va ma’lumotni tiklash manzilini qayergaligiga bog‘liq bo‘ladi. Qaysi jarayon | Ma’lumotlarni qayta tiklash |
|  | Antivirus dasturlarini ko’rsating? | Drweb, Nod32, Kaspersky |
|  | Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi | wep, wpa, wpa2 |
|  | Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak? | ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | bit |
|  | Virtual xususiy tarmoq – bu? | VPN |
|  | Xavfli viruslar bu - … | kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Rezident virus... | tezkor xotirada saqlanadi |
|  | DIR viruslari nimani zararlaydi? | FAT tarkibini zararlaydi |
|  | .... kompyuter tarmoqlari bo’yicha tarqalib, komlg’yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi | «Chuvalchang» va replikatorli virus |
|  | Mutant virus... | shifrlash va deshifrlash algoritmlaridan iborat- to’g’ri javob |
|  | Fire Wall ning vazifasi... | tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi |
|  | Kompyuter virusi nima? | maxsus yozilgan va zararli dastur |
|  | Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating | disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali |
|  | Troyan dasturlari bu... | virus dasturlar |
|  | Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? | 5 |
|  | Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud | detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya mahnosi... | sirli yozuv |
|  | …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi | K.Shennon |
|  | Kriptologiya yo’nalishlari nechta? | 2 |
|  | Kriptografiyaning asosiy maqsadi... | maxfiylik, yaxlitlilikni ta`minlash |
|  | Zararli dasturiy vositalarni aniqlash turlari nechta | 3 |
|  | Signaiurana asoslangan | ...bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
|  | O‘zgarishni aniqlashga asoslangan | Zararli dasturlar biror joyda joylashishi sababli, agar tizimdagi biror joyga o‘zgarishni aniqlansa, u holda u zararlanishni ko‘rsatishi mumkin |
|  | Anomaliyaga asoslangan | Noodatiy yoki virusga o‘xshash yoki potensial zararli harakatlari yoki xususiyatlarni topishni maqsad qiladi |
|  | Antiairuslar qanday usulda viruslarni aniqlaydi | Signaturaga asoslangan |
|  | Viruslar - | o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi |
|  | Rootkitlar- | ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi |
|  | Backdoorlar - | zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish |
|  | Troyan otlari- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Ransomware- | mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi |
|  | Resurslardan foydalanish usuliga ko’ra viruslar qanday turlarga bo’linadi | Virus parazit, Virus cherv |
|  | Zararlagan obyektlar turiga ko’ra | Dasturiy, yuklanuvchi, Makroviruslar, multiplatformali viruslar |
|  | Faollashish prinspiga ko’ra | Resident, Norezident |
|  | Dastur kodini tashkil qilish yondashuviga ko‘ra | Shifrlangan, shifrlanmagan, Polimorf |
|  | Shifrlanmagan viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang | 840 |
|  | 256mod25=? | 6 |
|  | bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi. | Tizim |
|  | Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima duyidadi | Xavfsizlik siyosati |
|  | RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday? |  |

|  |  |  |
| --- | --- | --- |
| *p* va *q* –sonlarning ko‘paytmasini ifodalovchi sonning spektoriga teng; | DES algoritmi akslantirishlari raundlari soni qancha? | 16; |
|  | DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha? | CHap qism blok 32 bit, o‘ng qism blok 32 bit; |
|  | Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? | SHifrlash va deshifrlash jarayonlari uchun kalitlarni generatsiya qilish qoidalariga ko‘ra farqlanadi |
|  | 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta? | 18 ta |
|  | 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta? | 4 ta |
|  | Eyler funsiyasida 𝜙(1) qiymati nimaga teng? | 0 |
|  | Eyler funksiyasida 60 sonining qiymatini toping. | 59 |
|  | Eyler funksiyasi yordamida 1811 sonining qiymatini toping. | 1810 |
|  | 97 tub sonmi? | Tub |
|  | Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256. | 244 |
|  | Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220 | 44 |
|  | Quyidagi ifodani qiymatini toping. -17mod11 | 5 |
|  | 2 soniga 10 modul bo’yicha teskari sonni toping. | Ø |
|  | Tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta’minlash sohasidagi tadbirlar tavsiflanadigan yuqori darajadagi reja nima? | Kiberxavfsizlik siyosati |
|  | Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi? | tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi |
|  | Kiberxavfsizlikni ta’minlash masalalari bo’yicha xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang | SANS (System Administration Networking and Security) |
|  | Korxonaning davomli muvaffaqiyat bilan faoliyat yuritishinita’minlashga mo’ljallangan strukturalangan va o’zaro bog’langan harakatlar to’plami- … | Strategiya |
|  | Tahdidlarning muvaffaqiyatli amalga oshirilishiga imkon beruvchi har qanday omil – bu … | Zaiflik |
|  | ISO/IEC 27002:2005 – …. | Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari |
|  | O’zDStISO/IEC 27005:2013 – …. | Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish |
|  | Axborot xavfsizligi arxitekturasining nechta satxi bor? | 3 |
|  | Rahbariy hujjat. Ma’lumotlar uzatish tarmog’ida axborot xavfsizligini ta’minlash to’g’risida Nizom - Xujjat raqamini toping | RH 45-215:2009 |
|  | Davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta’minlash dasturini ishlab chiqish tartibi - Xujjat raqamini toping | RH 45-185:2011 |
|  | Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta’minlash darajasini aniqlash tartibi - Xujjat raqamini toping | RH 45-193:2007 |
|  | Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta’riflar - Xujjat raqamini toping | TSt 45-010:2010 |
|  | Quyidagilardan qaysi standart aloqa va axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta’riflarni belgilaydi? | TSt 45-010:2010 |
|  | Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni nima? | Identifikatsiya |
|  | Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima? | Autentifikatsiya |
|  | Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni – nima deyiladi? | Avtorizatsiya |
|  | Identifikatsiya nima? | Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni |
|  | Autentifikatsiya nima? | Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni |
|  | Avtorizatsiya nima? | Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni |
|  | ... - Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o’tishni ta’minlovchi biror axborot | Parol |
|  | Smart karta o’lchamidagi, kichik xajmdagi xotira va xisoblash imkoniyatiga ega bo’lgan, o’zida parol yoki kalitni saqlovchi qurilma nima deb ataladi? | Token, Smartkarta |
|  | Smarkarta nima asosida autentifikatsiyalaydi? | Something you have |
|  | Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o’zgarib turadigan parol nima deyiladi? | One-time password (OTP) |
|  | Foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish nima deb ataladi? | Ma’murlash |
|  | Amaldagi qonunchilikka mos ravishda texnik, dasturiy va dasturiy-texnik vositalar yordamida axborot xavfsizligining nokriptografik usullari bilan ta’minlashni inobatga oluvchi axborot himoyasi nima? | Axborotning texnik himoyasi |
|  | Nazorat hududi – bu ... | Qo’riqlanuvchi soha bo’lib, uning ichida kommunikatsiya qurilmalari hamda axborot tarmog’ining lokal tarkibiy qurilmalarini birlashtiruvchi barcha nuqtalar joylashadi |
|  | Texnik himoya vositalari – bu ... | Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob’ektni himoyalashdir |
|  | Bu axborotni tutib olish qurilmasi bo’lib, ularda uzatuvchi qurilma sifatida kontaktli mikrofonlardan foydalaniladi | Stetoskoplar |
|  | Xesh funktsiya to’g’ri ko’rsatilgan javobni aniqlang. | MD5 |
|  | MD5, SHA1, Tiger xesh funktsiyalari uchun blok uzunligi necha baytga teng? | 64 bayt |
|  | Sub’ektni ob’ektga ishlash qobilyatini aniqlash – nima? | Foydalanishni boshqarish |
|  | Foydalanishni boshqarishda sub’ekt bu - .... | Inson, dastur, jarayon |
|  | Foydalanishni boshqarishning qaysi usuli tizimdagi shaxsiy ob’ektlarni ximoyalash uchun qo’llaniladi? | Discretionary access control DAC |
|  | Foydalanishni boshqarishning qaysi usulidan asosan operatsion tizimlarda qo’llaniladi? | Discretionary access control DAC |
|  | Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi? | Mandatory access control MAC |
|  | Foydalanishni boshqarishning qaysi usulida xavfsizlik markazlashgan tarzda xavfsizlik siyosati m’muri tomonidan amalga oshiriladi? | Mandatory access control MAC |
|  | Foydalanishni boshqarishning qaysi usulida xar bir foydalanuvchini foydalanish ruxsatini belgilash o’rniga rol uchun ob’ektlardan foydalanish ruxsatini ko’rsatish yetarli bo’ladi? | Role-based access control RBAC |
|  | Foydalanishni boshqarishning qaysi usulida sub’ekt va ob’ektlarga tegishli xuquqlarni ma’murlash oson kechadi? | Role-based access control RBAC |
|  | Firibgarlikni oldini olish uchun bir shaxs tomonidan ko’plab vazifalarni bajarishga ruxsat bermaslik zarur. Bu muammo foydalanishni boshqarishni qaysi usulida bartaraf etiladi? | Role-based access control RBAC |
|  | Ob’ekt va sub’ektlarning attributlari, ular bilan mumkin bo’lgan amallar va so’rovlarga mos keladigan muxit uchun qoidalarni taxlil qilish asosida foydalanishni boshqarish - .... | Attribute based access control ABAC |
|  | Attribute based access control ABAC usuli attributlari qaysilar? | Foydalanuvchi attributlari, Resurs attributlari, Ob’ekt va muxit attributlari |
|  | Foydalanishni boshqarishning qaysi usulida ruxsatlar va xarakatni kim bajarayotganligi to’g’risidagi xolatlar “agar, u xolda” buyrug’idan tashkil topgan qoidalarga asoslanadi? | Attribute based access control ABAC |
|  | XASML standarti foydalanishni boshqarishning qaysi usulida qo’llaniladi? | Attribute based access control ABAC |
|  | XASML standartida qoida nima? | Maqsad, ta’sir, shart, majburiyat va maslaxatlar |
|  | XASML standartida maqsad nima? | Sub’ekt ob’ekt ustida nima xarakat qilishi |
|  | Lampsonning foydalanishni boshqarish matritsasi nimalardan tashkil topgan? | Imtiyozlar ro’yxati |
|  | Access control list va Capability list bu nimaning asosiy elementi xisoblanadi? | Lampson matritsasining |
|  | Lampson matritsasining satrlarida nima ifodalanadi? | Sub’ektlar |
|  | Foydalanishni boshqarishning mantiqiy vositalari infratuzilma va uning ichidagi tizimlarda ... uchun foydalaniladi. | Mandat, Tasdiqlash, Avtorizatsiya |
|  | SHaxsiy simsiz tarmoq standartini aniqlang. | Bluetooth, IEEE 802.15, IRDA |
|  | Lokal simsiz tarmoq standartini aniqlang. | IEEE 802.11, Wi-Fi, HiperLAN |
|  | Regional simsiz tarmoq standartini aniqlang. | IEEE 802.16, WiMAX |
|  | Global simsiz tarmoq standartini aniqlang. | CDPD, 2G, 2.5G, 3G, 4G, 5G |
|  | Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang. | SHaxsiy simsiz tarmoq |
|  | IEEE 802.11, Wi-Fi, HiperLAN standartida ishlovchi simsiz tarmoq turini aniqlang. | Lokal simsiz tarmoq |
|  | IEEE 802.16, WiMAX standartida ishlovchi simsiz tarmoq turini aniqlang. | Regional simsiz tarmoq |
|  | CDPD, 2G, 2.5G, 3G, 4G, 5G standartida ishlovchi simsiz tarmoq turini aniqlang. | Global simsiz tarmoq |
|  | Bluetooth qanday chastota oralig’ida ishlaydi? | 2.4-2.485 Ggts |
|  | Wi-Fi qanday chastota oralig’ida ishlaydi? | 2.4-5 Ggts |
|  | WiMax tarmog’ining tezligi qancha? | 1 Gbit/sekund |
|  | Quyidagilardan qaysi biri MITM xujumiga tegishli xatti-xarakat ximoblanadi? | Aloqa seansini konfidentsialligini va yaxlitligini buzish |
|  | WiMAX tarmoq arxitekturasi nechta tashkil etuvchidan iborat? | 5 |
|  | WiMAX tarmoq arxitekturasi qaysi tashkil etuvchidan iborat? | Base station, Subscriber station, Mobile station, Relay station, Operator network |
|  | GSM raqamli mobil telefonlarining nechanchi avlodi uchun ishlab chiqilgan protokol? | Ikkinchi avlodi |
|  | GSM standarti qaysi tashkilot tomonidan ishlab chiqilgan? | European telecommunications standards institute |
|  | .... – o’zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma’lumoti va xavfsizlik algoritmlarini saqlaydi. | Sim karta |
|  | Rutoken S qurilmasining og’irligi qancha? | 6.3 gramm |
|  | True Crypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES, Serpent, Twofish |
|  | Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidentsialligini aniqlash qaysi dasturiy shifrlash vositalarining vazifasi? | Disc encryption software |
|  | BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES, Serpent, Twofish |
|  | AxCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES-256 |
|  | Qog’oz ko’rinishidagi axborotlarni yo’q qilish qurilmasining nomini kiriting. | Shreder |
|  | Ma’lumotlarni bloklarga bo’lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya? | RAID 0 |
|  | Qaysi texnologiyada ma’lumotni ko’plab nusxalari bir vaqtda bir necha disklarga yoziladi? | RAID 1 |
|  | Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi? | RAID 3 |
|  | Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi? | RAID 5 |
|  | Disk zararlanganda “qaynoq almashtirish” yordamida uni almashtirish mumkin. Bu xususiyat qaysi texnologiyaga tegishli? | RAID 50 |
|  | Zaxiralashning qanday turlari mavjud? | To’liq, o’sib boruvchi, differentsial |
|  | IOS, Android, USB xotiralardan ma’lumotlarni tiklash uchun qaysi dasturdan foydalaniladi? | EASEUS Data recovery wizard |
|  | Foydalanuvchi ma’lumotlarini qo’lga kirituvchi va uni xujumchiga yuboruvchi dasturiy kod nima? | Spyware |
|  | Operatsion tizim tomonidan aniqlanmasligi uchun ma’lum xarakatlarni yashirish nima deyiladi? | Rootkits |
|  | Qurbon kompyuterda mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo’yib to’lov amalga oshirishni talab qiladi. Bu qaysi zararli dastur? | Ransomware |
|  | Quyidagilardan o’zidan ko’payishi yo’q bo’lganlarini belgilang. | Mantiqiy bomba, Troyan oti, Backdoors |
|  | Viruslar resurslardan foydalanish usuliga ko’ra qanday turlarga bo’linadi? | Virus parazitlar, virus chervlar |
|  | Viruslar zararlangan ob’ektlar turiga ko’ra qanday turlarga bo’linadi? | Dasturiy, yuklanuvchi, makroviruslar, ko’p platformali |
|  | Viruslar faollashish printsipiga ko’ra qanday turlarga bo’linadi? | Rezident, norezident |
|  | Viruslar dastur kodini tashkil qilish yondoshuviga ko’ra qanday turlarga bo’linadi? | SHifrlangan, shifrlanmagan, polimorf |
|  | Dastlabki virus nechanchi yilda yaratilgan? | 1988 |
|  | ILOVEYOU virusi keltirgan zarar qancha? | 10 mlrd. Dollar |
|  | CodeRed virusi keltirgan zarar qancha? | 2 mlrd. Dollar |
|  | Melissa virusi keltirgan zarar qancha? | 80 million dollar |
|  | NetSky virusi keltirgan zarar qancha? | 18 mlrd. Dollar |
|  | MyDoom virusi keltirgan zarar qancha? | 38 mlrd. Dollar |
|  | Risk monitoring ….. ni paydo bo’lish imkoniyatini aniqlaydi. | Yangi risklar |
|  | ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi. | Risk monitoring |
|  | Axborot xavfsizligi siyoatining necha hil turi bor? | 3 |
|  | Internetdan foydalanish siyosatining nechta turi mavjud? | 4 |
|  | Nomuntazam siyosat (Promiscuous Policy) nima? | Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi |
|  | Paranoid siyosati (Paranoid Policy) – bu …. | Hamma narsa ta’qiqlanadi |
|  | Ruxsat berishga asoslangan siyosat (Permissive Policy) – bu … | Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi |
|  | Ehtiyotkorlik siyosati (Prudent Policy) – bu …. | Barcha hizmatlar blokirovka qilingandan so’ng bog’lanadi |
|  | Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi. Bu qaysi xavfsizlik siyosatiga hos? | Nomuntazam siyosat (Promiscuous Policy) |
|  | Barcha hizmatlar blokirovka qilingandan so’ng bog’lanadi. Bu qaysi xavfsizlik siyosatiga hos? | Ehtiyotkorlik siyosati (Prudent Policy) |
|  | Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi. Bu qaysi xavfsizlik siyosatiga hos? | Ruxsat berishga asoslangan siyosat (Permissive Policy) |
|  | Hamma narsa ta’qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos? | Paranoid siyosati (Paranoid Policy) |
|  | Tizim arxitekturasining turlari nechta? | 5 |
|  | Internet, havo hujumidan mudofaa, transport tizimlari qaysi tizim arxitekturasiga xos? | Hamkorlik tizimlari arxitekturasi |
|  | Cloud computing texnologiyasining nechta asosiy turi mavjud? | 3 |
|  | Raqamli soatlar qaysi texnologiyaga tegishli? | O’rnatilgan tizimlar (Embedde systems) |
|  | Xavfsizlikning asosiy yo’nalishlarini sanab o’ting. | \*Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik |
|  | Axborot xavfsizligining asosiy maqsadlaridan biri- bu… | \*Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish |
|  | Konfidentsiallikga to’g’ri ta`rif keltiring. | \*axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; |
|  | Yaxlitlikni buzilishi bu - … | \*Soxtalashtirish va o’zgartirish |
|  | ... axborotni himoyalash tizimi deyiladi. | \*Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi |
|  | Kompyuter virusi nima? | \*maxsus yozilgan va zararli dastur |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | \*kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya ma’nosi... | \*sirli yozuv |
|  | Kriptografiyaning asosiy maqsadi... | \*maxfiylik, yaxlitlilikni ta`minlash |
|  | SMTP - Simple Mail Transfer protokol nima? | \*elektron pochta protokoli |
|  | SKIP protokoli... | \*Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi |
|  | Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar… | \*uzilish, tutib qolish, o’zgartirish, soxtalashtirish |
|  | ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. | \*konfidentsiallik |
|  | Foydalanish huquqini cheklovchi matritsa modeli bu... | \*Bella La-Padulla modeli |
|  | Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? | \*TCP/IP, X.25 protokollar |
|  | Himoya tizimi kompleksligiga nimalar orqali erishiladi? | \*Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali |
|  | Kalit – bu … | \*Matnni shifrlash va shifrini ochish uchun kerakli axborot |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | \*simmetrik kriptotizimlar |
|  | Autentifikatsiya nima? | \*Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi |
|  | Identifikatsiya bu- … | \*Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni |
|  | O’rin almashtirish shifri bu - … | \*Murakkab bo’lmagan kriptografik akslantirish |
|  | Simmetrik kalitli shifrlash tizimi necha turga bo’linadi. | \*2 turga |
|  | Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular … | \*hosil qilish, yig’ish, taqsimlash |
|  | Kriptologiya - | \*axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi |
|  | Kriptografiyada alifbo – | \*axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam |
|  | Simmetrik kriptotizimlarda ... jumlani davom ettiring | \*shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi |
|  | Kriptobardoshlilik deb … | \*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Elektron raqamli imzo deb – | \*xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha |
|  | Kriptografiya – | \*axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi |
|  | Kriptografiyada matn – | \*alifbo elementlarining tartiblangan to’plami |
|  | Kriptoanaliz – | \*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Shifrlash – | \*akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi |
|  | Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi? | \*Tez, aniq va maxfiyligiga |
|  | Faol hujum turi deb… | \*Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon |
|  | Blokli shifrlash- | \*shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish |
|  | Simmetrik kriptotizmning uzluksiz tizimida … | \*ochiq matnning har bir harfi va simvoli alohida shifrlanadi |
|  | Kripto tizimga qo’yiladigan umumiy talablardan biri | \*shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak |
|  | Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos? | \*Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi |
|  | Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang | \*Vijener matritsasi, Sezar usuli |
|  | Akslantirish tushunchasi deb nimaga aytiladi? | \*1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga |
|  | Simmetrik guruh deb nimaga aytiladi? | \*O’rin almashtirish va joylashtirish |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | \*simmetrik kriptosistemalar |
|  | Xavfli viruslar bu - … | \*kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | \*Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi? | \*raqamli imzoni shakllantirish va tekshirish muolajasi |
|  | Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? | \*Simmetrik va assimetrik |
|  | Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin? | \*Korporativ va umumfoydalanuvchi |
|  | Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo’linadi? | \*Sust va faol |
|  | Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? | \*SMTP, POP yoki IMAR |
|  | Axborot resursi – bu? | \*axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi |
|  | Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu? | \*login |
|  | Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu? | \*parol |
|  | Identifikatsiya jarayoni qanday jarayon? | \* axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni |
|  | Autentifikatsiya jarayoni qanday jarayon? | \*obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash |
|  | Avtorizatsiya jarayoni qanday jarayon? | \*foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni |
|  | Ro’yxatdan o’tish bu? | \*foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni |
|  | Axborot qanday sifatlarga ega bo’lishi kerak? | \*ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | \*bit |
|  | Elektron hujjatning rekvizitlari nechta qismdan iborat? | \*4 |
|  | Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? | \*fleshka, CD va DVD disklar |
|  | Imzo bu nima ? | \*hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati. |
|  | Muhr bu nima? | \*hujjatning haqiqiyligini va biror bir yuridik shaxsga tegishli ekanligini tasdiqlovchi isbotdir |
|  | DSA – nima | \*Raqamli imzo algoritmi |
|  | El Gamal algoritmi qanday algoritm | \*Shifrlash algoritmi va raqamli imzo algoritmi |
|  | Sezarning shifrlash sistemasining kamchiligi | \*Harflarning so’zlarda kelish chastotasini yashirmaydi |
|  | Axborot xavfsizligi va xavfsizlik san’ati haqidagi fan …. deyiladi? | \*Kriptografiya |
|  | Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu - | \*steganografiya |
|  | Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? | \*Deshifrlash |
|  | …… – hisoblashga asoslangan bilim sohasi bo‘lib,  buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. | \*Kiberxavfsizlik |
|  | Risk | \*Potensial foyda yoki zarar |
|  | Tahdid nima? | \*Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
|  | Kodlash nima? | \*Ma’lumotni osongina qaytarish uchun hammaga  ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir |
|  | Shifrlash nima? | Ma’lumotni osongina qaytarish uchun hammaga  ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir |
|  | Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi | Kriptoanaliz |
|  | Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi | {*d, e*} – ochiq, {*e, n*} – yopiq; |
|  | Zamonaviy kriptografiya qanday bo’limlardan iborat? | Electron raqamli imzo; kalitlarni boshqarish |
|  | Kriptografik usullardan foydalanishning asosiy yo’nalishlari nimalardan iborat? | uzatiliyotgan xabarlarni haqiqiyligini aniqlash |
|  | Shifr nima? | \* Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm |
|  | Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? | \*Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi |
|  | Oqimli shifrlashning mohiyati nimada? | Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,  Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi |
|  | Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating. | \*uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim, |
|  | Kriptotizim qaysi komponentlardan iborat? | \*ochiq matnlar fazosi M, Kalitlar fazosi K,  Shifrmatnlar fazosi C, Ek : M → C (shifrlash uchun) va Dk: C→M (deshifrlash uchun) funktsiyalar |
|  | Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? | \*shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun |
|  | Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi. | \*ochiq kalitlar |
|  | Xesh-funktsiyani natijasi … | Kiruvchi xabar uzunligidan uzun xabar |
|  | RSA algoritmi qanday jarayonlardan tashkil topgan | \*Kalitni generatsiyalash; Shifrlash; Deshifrlash. |
|  | Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi | \*Xesh funksiyalar |
|  | To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub | \*Xalqa |
|  | Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo’llamasligi mumkin? | \*to’liq bog’lanishli |
|  | Kompyuterning tashqi interfeysi deganda nima tushuniladi? | \*kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari |
|  | Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? | \*Yulduz |
|  | Ethernet kontsentratori qanday vazifani bajaradi | \*kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi |
|  | OSI modelida nechta satx mavjud | \*7 |
|  | OSI modelining to’rtinchi satxi qanday nomlanadi | \*Transport satxi |
|  | OSI modelining beshinchi satxi qanday nomlanadi | \*Seanslar satxi |
|  | OSI modelining birinchi satxi qanday nomlanadi | \*Fizik satx |
|  | OSI modelining ikkinchi satxi qanday nomlanadi | \*Kanal satxi |
|  | OSI modelining uchinchi satxi qanday nomlanadi | \*Tarmoq satxi |
|  | OSI modelining oltinchi satxi qanday nomlanadi | \*Taqdimlash satxi |
|  | OSI modelining yettinchi satxi qanday nomlanadi | \*Amaliy satx |
|  | OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi | \*fizik, kanal va tarmoq satxlari |
|  | OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi | \*Marshrutizator |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi | \*Fizik satx |
|  | Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi | \*Tarmoq satxi |
|  | Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub | \*IP, IPX |
|  | Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub | \*TCP,UDP |
|  | OSI modelining fizik satxi qanday funktsiyalarni bajaradi | \*Elektr signallarini uzatish va qabul qilish |
|  | OSI modelining amaliy satxi qanday funktsiyalarni bajaradi | \*Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub | \*Ethernet, FDDI |
|  | Keltirilgan protokollarning qaysilari taqdimlash satxi protokollariga mansub | \*SNMP, Telnet |
|  | Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu... | \*Avtorizatsiya |
|  | Autentifikatsiya faktorlari nechta | 4 |
|  | Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima | Login |
|  | Ko‘z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar? | Biron nimaga egalik asosida |
|  | barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi? | \*Fizik satx |
|  | Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi | \*2 |
|  | Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? | \*Foydalanishni boshqarish |
|  | Foydalanishni boshqarish –bu... | Subyektni Subyektga ishlash qobilyatini aniqlashdir. |
|  | Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi? | Obyekt |
|  | Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ? | \*Obyekt |
|  | Foydalanishna boshqarishning nechta usuli mavjud? | \*4 |
|  | Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo‘llaniladi | ABAC |
|  | Foydalanishni boshqarishning qaysi modelida Obyekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi | ABAC |
|  | Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi. | ABAC |
|  | Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bog‘liq.. | Tashkilotda Obyektning muhimlik darajasi bilan yoki yuzaga keladigan foyda miqdori bilan bilan xarakterlanadi |
|  | MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi | \*xavfsizlik siyosati ma’muri |
|  | Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi | Yozish |
|  | Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi. | \*Yozish |
|  | Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun Obyektlardan foydalanish ruxsati ko‘rsatiladi? | ABAC |
|  | Rol tushunchasiga ta’rif bering. | \*Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin |
|  | Foydalanishni boshqarishning qaysi usuli - Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. | \*ABAC |
|  | XACML foydalanishni boshqarishni qaysi usulining standarti? | \*ABAC |
|  | Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan? | \*barchasi |
|  | Axborotning kriptografik himoya vositalari necha turda? | 4 |
|  | Dasturiy shifrlash vositalari necha turga bo‘linadi | \*4 |
|  | Diskni shifrlash nima uchun amalga oshiriladi? | \*Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi |
|  | Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi? | 8 |
|  | Kompyuter tarmoqlari bu – | \*Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi |
|  | Tarmoq modeli –bu.. ikki | Matematik modellar to‘plami |
|  | OSI modelida nechta tarmoq satxi bor | \*7 |
|  | OSI modeli 7 satxi bu | \*Ilova |
|  | OSI modeli 1 satxi bu | Ilova |
|  | OSI modeli 2 satxi bu | Ilova |
|  | TCP/IP modelida nechta satx mavjud | \*4 |
|  | Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi? | Lokal |
|  | Tarmoq kartasi bu... | \*Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Switch bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Hab bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Tarmoq repiteri bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi. | \*DNS tizimlari |
|  | ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. | \*TCP |
|  | …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi. | \*UDP |
|  | Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi. | TCP |
|  | Tarmoq taxdidlari necha turga bo‘linadi | 2 |
|  | Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; | \*Razvedka hujumlari |
|  | Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi | Razvedka hujumlari |
|  | Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi; | Razvedka hujumlari |
|  | Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi; | Razvedka hujumlari |
|  | RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart? | \*e soni Eyler funksiyasi - bilan o‘zaro tub |
|  | RSA elektron raqamli imzo algoritmidagi yopiq kalit  d qanday hisoblanadi? Bu yerda p va q tub sonlar,n=pq, - Eyler funksiyasi,e-ochiq kalit | \* |
|  | Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? | \*Imzo qo‘yish va imzoni tekshirishdan |
|  | Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? | \*Imzo muallifining ochiq *kaliti yordamida* |
|  |  |  |

|  |
| --- |
| **Tarmoq modeli-bu...** |
| \*Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar  muvaffaqqiyatli o‘rnatilishini asosidir |
|  | OSI modeli nechta satxga ajraladi? | 2 |
|  | Fizik satxning vazifasi nimadan iborat | \*Qurilma, signal va binar o‘zgartirishlar |
|  | Ilova satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | Kanal satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | Tarmoq satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | TCP/IP modeli nechta satxdan iborat | \*4 |
|  | Quyidagilarninf qaysi biri Kanal satxi protokollari | \*Ethernet, Token Ring, FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri tarmoq satxi protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri transport satxi protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri ilova satxi protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi | \*Kanal, Fizik |
|  | TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi | Kanal, Fizik |
|  | TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi | Kanal, Fizik |
|  | TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos keladi | Kanal, Fizik |
|  | Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang. | \*Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan | \*Tarmoqda har bir kompyuter yoki tugun Markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Tarmoq kartasi nima? | \*Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Repetir nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Hub nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Switch nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Router nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | DNS tizimlari. | \*Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi |
|  | TCP bu- … | \*Transmission Control Protocol |
|  | UDP bu-… | User domain protocol |
|  | IP protokolining necha xil versiyasi mavjud? | 1 |
|  | Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang | \*Ichki, tashqi |
|  | Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi | \*Biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi | \*Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya  usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya  usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi | \*Razvedka hujumlari |
|  | Razvedka hujumiga berilgan ta’rifni aniqlang | \*Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
|  | Kirish hujumiga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axboro ni to‘plashni maqsad qiladi; |
|  | DOS hujumiga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
|  | Zararli hujumga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
|  | Razvetka hujumari necha turga bo’linadi | 1 |
|  | Qaysi hujum jarayoni TCP/IP tarmog‘ida paketlarni tutib  olish, dekodlash, tekshirish va tarjima qilishni o‘z ichiga  oladi | \*Paketlarni snifferlash |
|  | Tarmoqlaro ekranni OSI modeli bo’yicha qanday turlarga bo’lindi? | \*• paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida |
|  | Tarmoqlaro ekranni foydalanilgan texnologiyasi bo’yicha qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida |
|  | Tarmoqlaro ekranni bajarilishiga ko’ra qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida |
|  | Tarmoqlaro ekranni ulanish sxemasi bo’yicha qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahidaishlaydi; ilova proksilari – ilova satxida |
|  | Paket filtrlari tarmoqlararo ekrani vazifasi nima? | \*Tarmoq satxida paketlarni  tahlillashga asoslan; |
|  | Ilova proksilari tarmoqlararo ekrani vazifasi nima? | Tarmoq satxida paketlarni tahlillashga asoslan; |
|  | Ekspert paket filtrlari tarmoqlararo ekrani vazifasi nima? | Tarmoq satxida paketlarni tahlillashga asoslan; |
|  | Quyidagilardan qaysi biri paket filtrlari tarmoqlararo ekrani kamchiligini ifodalaydi. | \*Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma’lumotlarni, zararli dasturlarni va hak. tekshirmaydi. |
|  | Quyidagilardan qaysi biri ekspert paket filtrlari tarmoqlararo ekrani kamchiligini ifodalaydi. | Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma’lumotlarni, zararli  dasturlarni va hak. tekshirmaydi. |
|  | Simsiz tarmoqlarning nechta turi mavjud | 5 |
|  | Bluetooth qanday simsiz tarmoq turiga kiradi. | Global |
|  | Wifi qanday simsiz tarmoq turiga kiradi. | Global |
|  | LTE, CDMA, HSDPA qanday simsiz tarmoq turiga kiradi. | \*Global |
|  | WiMAX qanday simsiz tarmoq turiga kiradi. | Global |
|  | Bluetooth texnologiyasida autentifikatsiya bu… | Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. |
|  | Bluetooth texnologiyasida konfidensiallik bu… | \*Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. |
|  | Bluetooth texnologiyasida avtorizatsiya bu… | Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. |
|  | GSM bu ..- | \*Global System for Mobile Communications |
|  | Simsiz tarmoq Bluetooth ishlash rejimlari nechta? | 2 |
|  | Kompyuterda hodisalar haqidagi ma’lumot qayerda saqlanadi? | \*hodisalar jurnaliga |
|  | Windows operatsion tizimida xatolik hodisasiga berilgan ta’rifni belgilang. | \*Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
|  | Windows operatsion tizimida ogohlantirish hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
|  | Windows operatsion tizimida axborot hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
|  | Windows operatsion tizimida muvaffaqiyatli audit hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
|  | Windows operatsion tizimida muvaffaqiyatsiz audit hodisasiga berilgan ta’rifni belgilang. | Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi. |
|  | Ma’lumotlarni zaxira nusxalash bu – … | \*Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi |
|  | Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz | \*Zaxira nusxalash |
|  | Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering | \*Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Ma’lumotlarni g’arazli hatti harakatlar yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Ma’lumotlarni tasodifiy sabablar tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Ma’lumotlarni tabiiy ofatlar tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi? | 7 |
|  | Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. | \*4 |
|  | Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash | \*Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | Zaxira nusxalovchi vositalar tanlashdagi *ishonchlilik* xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | Zaxira nusxalovchi vositalar tanlashdagi tezlik xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | Zaxira nusxalovchi vositalar tanlashdagi foydalanuvchanlik xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | Zaxira nusxalovchi vositalar tanlashdagi qulaylik xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | RAID texnologiyasining transkripsiyasi qanday. | Redundant Array of Independent Disks |
|  | RAID texnologiyasida nechta satx mavjud | 3 |
|  | RAID 0: diskni navbatlanishi bu-.. | \*Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi. Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
|  | RAID 1: diskni navbatlanishi bu-.. | Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi.  Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
|  | RAID 3: diskni navbatlanishi bu-.. | Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi.  Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
|  | RAID 5: diskni navbatlanishi bu-.. | Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi.  Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi |
|  | RAID 10: diskni navbatlanishi bu-.. | \*Gibrid satx bo‘lib, RAID 1 va RAID 0  satxlaridan iborat va kamida 4 ta diskni talab etadi |
|  | RAID 50: diskni navbatlanishi bu-.. | Gibrid satx bo‘lib, RAID 1 va RAID 0  satxlaridan iborat va kamida 4 ta diskni talab etadi |
|  | Ma’lumotlarni nusxalash usullari necha xil usulda amalga oshiriladi? | \*3 |
|  | Issiq zaxiralash usuliga berilgan ta’rifni belgilang. | \*Ushbu usulda foydalanuvchi tizimni boshqarayotgan  vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.  Mazkur zaxiralash usulini amalga oshirish tizimni  harakatsiz vaqtini kamaytiradi. |
|  | Iliq zaxiralash usuliga berilgan ta’rifni belgilang. | Ushbu usulda foydalanuvchi tizimni boshqarayotgan  vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.  Mazkur zaxiralash usulini amalga oshirish tizimni  harakatsiz vaqtini kamaytiradi. |
|  | Sovuq zaxiralash usuliga berilgan ta’rifni belgilang. | Ushbu usulda foydalanuvchi tizimni boshqarayotgan  vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.  Mazkur zaxiralash usulini amalga oshirish tizimni  harakatsiz vaqtini kamaytiradi. |
|  | Ichki zahiralash qanday amalga oshiriladi | Ichki zahiralashda mahalliy yoki global serverlardan foydalaniladi |
|  | OSI modelining birinchi satxi qanday nomlanadi | \*Fizik satx |
|  | OSI modelining ikkinchi satxi qanday nomlanadi | \*Kanal satxi |
|  | OSI modelining uchinchi satxi qanday nomlanadi | \*Tarmoq satxi |
|  | OSI modelining oltinchi satxi qanday nomlanadi | \*Taqdimlash satxi |
|  | OSI modelining ettinchi satxi qanday nomlanadi | \*Amaliy satx |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi | \*Fizik satx |
|  | Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub | \*TCP,UDP |
|  | OSI modelining fizik satxi qanday funktsiyalarni bajaradi | \*Elektr signallarini uzatish va qabul qilish |
|  | OSI modeliningamaliy satxi qanday funktsiyalarni bajaradi | \*Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | 12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan sonlar soni nechta? | 6 ta |
|  | Yevklid algoritmi qanday natijani beradi? | \*Sonning eng katta umumiy bo’luvchisini toppish |
|  | Qanday sonlar tub sonlar deb yuritiladi? | \*Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi. |
|  | To‘liq zaxiralash | Tiklashning tezligi yuqori. axira nusxalash jarayonining sekin va ma’lumotni saqlash  uchun ko‘p hajm talab etadi |
|  | O‘sib boruvchi zaxiralash | Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi |
|  | Differnsial zaxiralash | Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi |
|  | Ushbu jarayon ma’lumot qanday yo‘qolgani, ma’lumotni qayta tiklash dasturiy vositasi va ma’lumotni tiklash anzilini qayergaligiga bog‘liq bo‘ladi. Qaysi jarayon | Ma’lumotlarni qayta tiklash |
|  | Antivirus dasturlarini ko’rsating? | \*Drweb, Nod32, Kaspersky |
|  | Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi | \*wep, wpa, wpa2 |
|  | Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak? | \*ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | \*bit |
|  | Virtual xususiy tarmoq – bu? | \*VPN |
|  | Xavfli viruslar bu - … | \*kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | \*Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Rezident virus... | \*tezkor xotirada saqlanadi |
|  | DIR viruslari nimani zararlaydi? | \*FAT tarkibini zararlaydi |
|  | .... kompyuter tarmoqlari bo’yicha tarqalib, kompyuterning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi | \*«Chuvalchang» va replikatorli virus |
|  | Mutant virus... | \*shifrlash va deshifrlash algoritmlaridan iborat |
|  | Fire Wall ning vazifasi... | \*tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi |
|  | Kompyuter virusi nima? | \*maxsus yozilgan va zararli dastur |
|  | Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating | \*disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali |
|  | Troyan dasturlari bu... | \*virus dasturlar |
|  | Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? | \*5 |
|  | Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud | \*detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | \*kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya mahnosi... | \*sirli yozuv |
|  | …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi | \*K.Shennon |
|  | Kriptologiya yo’nalishlari nechta? | \*2 |
|  | Kriptografiyaning asosiy maqsadi... | \*maxfiylik, yaxlitlilikni ta`minlash |
|  | Zararli dasturiy vositalarni aniqlash turlari nechta | \*3 |
|  | Signaiurana asoslangan | \*....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh  qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
|  | O‘zgarishni aniqlashga asoslangan | ....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh  qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
|  | Anomaliyaga asoslangan | ....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh  qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
|  | Antiairuslar qanday usulda viruslarni aniqlaydi | Anomaliyaga asoslangan |
|  | Viruslar - | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Rootkitlar- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Backdoorlar - | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vositasifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Troyan otlari- | \*bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Ransomware- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Resurslardan foydalanish usuliga ko’ra viruslar qanday turlarga bo’linadi | \*Virus parazit, Virus cherv |
|  | Zararlagan obyektlar turiga ko’ra | Virus parazit, Virus cherv |
|  | Faollashish prinspiga ko’ra | Virus parazit, Virus cherv |
|  | Dastur kodini tashkil qilish yondashuviga ko‘ra | Virus parazit, Virus cherv |
|  | Shifrlanmagan viruslar | \*o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | Shifrlangan viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | Polimorf viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | Dasturiy viruslar-… | bir vaqtning o‘zida turli xildagi Obyektlarni  zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. |
|  | Ko‘p platformali viruslar | \*bir vaqtning o‘zida turli xildagi Obyektlarni  zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. |
|  | Yuklanuvchi viruslar | bir vaqtning o‘zida turli xildagi Obyektlarni  zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. |
|  | Makroviruslar-... | bir vaqtning o‘zida turli xildagi Obyektlarni  zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. |
|  | Birinchi kompyuter virusi nima deb nomlangan | Cherv |
|  | P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang | \*840 |
|  | 256mod25=? | 5 |
|  | bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi. | \*Tizim |
|  | Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori satxli hujjat yoki hujjatlar to‘plami nima duyidadi | Standart |
|  | RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday? | 65535; |
|  | DES algoritmi akslantirishlari raundlari soni qancha? | \*16; |
|  | DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha? | CHap qism blok 32 bit, o‘ng qism blok 48 bit; |
|  | Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? | SHifrlash va deshifrlash jarayonlarida kalitlardan foydalanish qoidalariga ko‘ra farqlanadi |
|  | 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta? | 19 ta |
|  | 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta? | \*4 ta |
|  | Qaysi formula qoldiqli bo’lish qonunini ifodalaydi |  |
|  | Eyler funsiyasida 𝜙(1) qiymati nimaga teng? | \*0 |
|  | Eyler funksiyasida 60 sonining qiymatini toping. | 59 |
|  | Eyler funksiyasi yordamida 1811 sonining qiymatini toping. | \*1810 |
|  | 97 tub sonmi? | \*Tub |
|  | Quyidagi modulli ifodani qiymatini toping  (148 + 14432) mod 256. | \*244 |
|  | Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220 | 21 |
|  | Quyidagi ifodani qiymatini toping.  -17mod11 | 6 |
|  | 2 soniga 10 modul bo’yicha teskari sonni toping. | 3 |

1. I:
2. S: Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.
3. +: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik
4. -: Axborot va Iqtisodiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xafvsizligi, Dasturiy ta`minot xavfsizligi
5. -: Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xafvsizligi, Ekologik xavfsizlik
6. -: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Dasturiy ta`minot xavfsizligi, Ekologik xavfsizlik
7. I:
8. S: Axborot xavfsizligining asosiy maqsadlaridan biri- bu…
9. +: Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish
10. -:Ob`yektga bevosita ta`sir qilish
11. -: Axborotlarni shifrlash, saqlash, yetkazib berish
12. -: Tarmoqdagi foydalanuvchilarni xavfsizligini ta`minlab berish
13. I:
14. S: Konfidentsiallikga to’g’ri ta`rif keltiring.
15. +: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
16. -:axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati;
17. -:axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati;
18. -:axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati;
19. I:
20. S: Yaxlitlikni buzilishi bu - …
21. +: Soxtalashtirish va o’zgartirish
22. -: Ishonchsizlik va soxtalashtirish
23. -: Soxtalashtirish
24. -: Butunmaslik va yaxlitlanmaganlik
25. I:
26. S:... axborotni himoyalash tizimi deyiladi.
27. +: Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi
28. -: Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo’qotilishidan keladigan zarar va himoyalash mexanizmining narxidan kelib chiqqan holda axborotni himoyalashning zaruriy darajasi
29. -: Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo’qotilishidan keladigan zarar va himoyalash mexanizmining zaruriy darajasi hamda tizimning turini, himoyalash usullar va vositalari
30. -: Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul
31. I:
32. S: Kompyuter virusi nima?
33. +: maxsus yozilgan va zararli dastur
34. -:.exe fayl
35. -: boshqariluvchi dastur
36. -: Kengaytmaga ega bo’lgan fayl
37. I:
38. S: Kriptografiyaning asosiy maqsadi...
39. +: maxfiylik, yaxlitlilikni ta`minlash
40. -:ishonchlilik, butunlilikni ta`minlash
41. -:autentifikatsiya, identifikatsiya
42. -:ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya
43. I:
44. S: SMTP - Simple Mail Transfer protokol nima?
45. +: elektron pochta protokoli
46. -:transport protokoli
47. -:internet protokoli
48. -:Internetda ommaviy tus olgan dastur
49. I:
50. S: SKIP protokoli...
51. +: Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi
52. -:Protokollar boshqaruvi
53. -:E-mail protokoli
54. -:Lokal tarmoq protokollari uchun kriptokalitlarning oddiy boshqaruvi
55. I:
56. S: Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar…
57. +: uzilish, tutib qolish, o’zgartirish, soxtalashtirish
58. -:o’zgartirish, soxtalashtirish
59. -:tutib qolish, o’zgarish, uzilish
60. -:soxtalashtirish, uzilish, o’zgartirish
61. I:
62. S: ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.
63. +: konfidentsiallik
64. -:identifikatsiya
65. -:autentifikatsiya
66. -: maxfiylik
67. I:
68. S: Foydalanish huquqini cheklovchi matritsa modeli bu...
69. +: Bella La-Padulla modeli
70. -:Dening modeli
71. -:Landver modeli
72. -:Huquqlarni cheklovchi model
73. I:
74. S: Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi?
75. +: TCP/IP, X.25 protokollar
76. -:X.25 protokollar
77. -:TCP/IP
78. -:SMTP
79. I:
80. S: Autentifikatsiya nima?
81. +: Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi
82. -: Tizim meyoriy va g’ayritabiiy hollarda rejalashtirilgandek o’zini tutishligi holati
83. -: Istalgan vaqtda dastur majmuasining mumkinligini kafolati
84. -:Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi
85. I:
86. S:Identifikatsiya bu- …
87. +: Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni
88. -:Ishonchliligini tarqalishi mumkin emasligi kafolati
89. -:Axborot boshlang’ich ko’rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o’zgarishlar
90. -:Axborotni butunligini saqlab qolgan holda uni elementlarini o’zgartirishga yo’l qo’ymaslik
91. I:
92. S:O’rin almashtirish shifri bu - …
93. +: Murakkab bo’lmagan kriptografik akslantirish
94. -:Kalit asosida generatsiya qilish
95. -:Ketma-ket ochiq matnni ustiga qo’yish
96. -:Belgilangan biror uzunliklarga bo’lib chiqib shifrlash
97. I:
98. S:Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.
99. +: 2 turga
100. -:3 turga
101. -:4 turga
102. -: 5 turga
103. I:
104. S: Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular …
105. +: hosil qilish, yig’ish, taqsimlash
106. -:ishonchliligi, maxfiyligi, aniqligi
107. -:xavfsizlik, tez ishlashi, to’g’ri taqsimlanishi
108. -:abonentlar soni, xavfsizligi, maxfiyligi
109. I:
110. S: Kriptologiya -
111. +: axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
112. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
113. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
114. -:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
115. I:
116. S: Kriptografiyada alifbo –
117. +: axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
118. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
119. -:xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
120. -:kalit axborotni shifrlovchi kalitlar
121. I:
122. S: Simmetrik kriptotizimlarda ... jumlani davom ettiring
123. +: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi
124. -:bir-biriga matematik usullar bilan bog’langan ochiq va yopiq kalitlardan foydalaniladi
125. -:axborot ochiq kalit yordamida shifrlanadi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi
126. -:kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi
127. I:
128. S: Kriptobardoshlilik deb …
129. +: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
130. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
131. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
132. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
133. I:
134. S: Elektron raqamli imzo deb –
135. +: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
136. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
137. -:axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
138. -:kalit axborotni shifrlovchi kalitlar
139. I:
140. S: Kriptografiya –
141. +: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
142. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
143. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
144. -:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
145. I:
146. S: Kriptografiyada matn –
147. +: alifbo elementlarining tartiblangan to’plami
148. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
149. -:axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
150. -:kalit axborotni shifrlovchi kalitlar
151. I:
152. S: Kriptoanaliz –
153. +: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
154. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
155. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
156. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
157. I:
158. S: Shifrlash –
159. +: akslantirish jarayoni ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi
160. -:kalit asosida shifrmatn ochiq matnga akslantiriladi
161. -:shifrlashga teskari jarayon
162. -:Almashtirish jarayoni bo’lib: ochiq matn deb nomlanadigan matn o’girilgan holatga almashtiriladi
163. I:
164. S: Faol hujum turi deb…
165. +: Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon
166. -:Maxfiy ma`lumotni aloqa tarmog’ida uzatilayotganda eshitish, tahrir qilish, yozib olish harakatlaridan iborat uzatilalayotgan ma`lumotni qabul qiluvchiga o’zgartirishsiz yetkazish jarayoni
167. -:Ma`lumotga o’zgartirish kiritmay uni kuzatish jarayoni
168. -:Sust hujumdan farq qilmaydigan jarayon
169. I:
170. S: Blokli shifrlash-
171. +: shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish
172. -:murakkab bo’lmagan kriptografik akslantirish
173. -:axborot simvollarini boshqa alfavit simvollari bilan almashtirish
174. -:ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi
175. I:
176. S: Simmetrik kriptotizmning uzluksiz tizimida …
177. +: ochiq matnning har bir harfi va simvoli alohida shifrlanadi
178. -:belgilangan biror uzunliklarga teng bo’linib chiqib shifrlanadi
179. -:murakkab bo’lmagan kriptografik akslantirish orqali shifrlanadi
180. -:ketma-ket ochiq matnlarni o’rniga qo’yish orqali shifrlanadi
181. I:
182. S: Kriptotizimga qo’yiladigan umumiy talablardan biri
183. +: shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak
184. -:shifrlash algoritmining tarkibiy elementlarini o’zgartirish imkoniyati bo’lishi lozim
185. -:ketma-ket qo’llaniladigan kalitlar o’rtasida oddiy va oson bog’liqlik bo’lishi kerak
186. -:maxfiylik o’ta yuqori darajada bo’lmoqligi lozim
187. I:
188. S: Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?
189. +: Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi
190. -:Asimmetrik tizimlarda k1=k2 bo’ladi, yahni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi
191. -:Asimmetrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma`lum bo’ladi, ochiq kalitni esa faqat qabul qiluvchi biladi
192. -:Asimmetrik kriptotizimlarda k1≠k2 bo’lib, kalitlar hammaga oshkor etiladi
193. I:
194. S: Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang
195. +: Vijener matritsasi, Sezar usuli
196. -:monoalfavitli almashtirish
197. -:polialfavitli almashtirish
198. -:o’rin almashtirish
199. I:
200. S: Akslantirish tushunchasi deb nimaga aytiladi?
201. +: 1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga
202. -:1-to’plamli elementlariga 2-to’plam elementalrini qarama-qarshiligiga
203. -:har bir elementni o’ziga ko’payimasiga
204. -:agar birinchi va ikinchi to’plam bir qiymatga ega bulmasa
205. I:
206. S: Simmetrik guruh deb nimaga aytiladi?
207. +: O’rin almashtirish va joylashtirish
208. -:O’rin almashtirish va solishtirish
209. -:Joylashtirish va solishtirish
210. -:O’rin almashtirish va transportizatsiyalash
211. I:
212. S: Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?
213. +: simmetrik kriptosistemalar
214. -:assimetrik kriptosistemalar
215. -:ochiq kalitli kriptosistemalar
216. -:autentifikatsiyalash
217. I:
218. S: Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?
219. +: SMTP, POP yoki IMAP
220. -:SKIP, ATM, FDDI
221. -:X.25 va IMAR
222. -:SMTP, TCP/IP
223. I:
224. S: Axborot resursi – bu?
225. +: axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi
226. -:cheklanmagan doiradagi shaxslar uchun mo’ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar
227. -:identifikatsiya qilish imkonini beruvchi rekvizitlari qo’yilgan holda moddiy jismda qayd etilgan axborot
228. -:manbalari va taqdim etilish shaklidan qathi nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to’g’risidagi ma`lumotlar
229. I:
230. S: Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu?
231. +: login parol
232. -:identifikatsiya
233. -:maxfiy maydon
234. -: token
235. I:
236. S: Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu?
237. +: parol
238. -:login
239. -:identifikatsiya
240. -:maxfiy maydon foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
241. I:
242. S: Identifikatsiya jarayoni qanday jarayon?
243. +: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
244. -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
245. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
246. -:foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
247. I:
248. S: Autentifikatsiya jarayoni qanday jarayon?
249. +: obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
250. -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
251. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
252. -:foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
253. I:
254. S: Ro’yxatdan o’tish bu?
255. +: foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
256. -:axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
257. -:ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
258. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
259. I:
260. S: Axborot qanday sifatlarga ega bo’lishi kerak?
261. +: ishonchli, qimmatli va to’liq
262. -:uzluksiz va uzlukli
263. -:ishonchli, qimmatli va uzlukli
264. -:ishonchli, qimmatli va uzluksiz
265. I:
266. S: Axborotning eng kichik o’lchov birligi nima?
267. +: bit
268. -:kilobayt
269. -:bayt
270. -:bitta simvol
271. I:
272. S: Elektron hujjatning rekvizitlari nechta qismdan iborat?
273. +: 4
274. -:5
275. -:6
276. -:7
277. I:
278. S: Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?
279. +: fleshka, CD va DVD disklar
280. -:Qattiq disklar va CDROM
281. -:CD va DVD, DVDROM
282. -:Qattiq disklar va DVDROM
283. I:
284. S: Avtorizatsiya jarayoni qanday jarayon?
285. +: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
286. -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va -berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
287. -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash.
288. -: parollash jarayoni
289. I:
290. S: Kodlash nima?
291. +: Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir
292. -:Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi
293. mumkin bo‘ladi
294. -:Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi
295. mumkin bo‘ladi
296. -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi
297. I:
298. S: Shifrlash nima?
299. +: Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi
300. -:Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir
301. -: Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi
302. -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi
303. I:
304. S: Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi
305. +:Kriptoanaliz
306. -:Kartografiya
307. -:Kriptologiya
308. -:Adamar usuli
309. I:
310. S: Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi
311. +: {d, n} – yopiq, {e, n} – ochiq;
312. -:{d, e} – ochiq, {e, n} – yopiq;
313. -:{e, n} – yopiq, {d, n} – ochiq;
314. -:{e, n} – ochiq, {d, n} – yopiq;
315. I:
316. S: Zamonaviy kriptografiya qanday bo’limlardan iborat?
317. -:Electron raqamli imzo; kalitlarni boshqarish
318. -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;
319. +: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish
320. -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; kalitlarni boshqarish
321. I:
322. S: Shifr nima?
323. +: Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm
324. -:Kalitlarni taqsimlash usuli
325. -:Kalitlarni boshqarish usuli
326. -:Kalitlarni generatsiya qilish usuli
327. I:
328. S: Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?
329. +: Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi
330. -:Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi
331. -:Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin
332. -:Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat deshifrlash mumkin
333. I:
334. S: Oqimli shifrlashning mohiyati nimada?
335. +: Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,
336. -:Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur,
337. -:Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi
338. -:Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,
339. I:
340. S: Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating.
341. +: uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim,
342. -:uzatilayotgan xabarni xavfsizligi kalitni maxfiyligiga emas, balki algoritmni maxfiyligiga bog’liq bo’lishi lozim
343. -:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog’liq bo’lishi lozim
344. -:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga emas, balki shifrlashda foydalaniladigan arifmetik amallar soniga bog’liq bo’lishi lozim
345. I:
346. S: Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?
347. +: shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun
348. -:ERI yaratish va tekshirish, kalitlar almashish uchun
349. -:shifrlash, deshifrlash, kalitlar almashish uchun
350. -: Heshlash uchun
351. I:
352. S: Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi.
353. +: ochiq kalitlar
354. -:yopiq kalitlar
355. -:seans kalitlari
356. -:Barcha tutdagi kalitlar
357. I:
358. S: Kompyuterning tashqi interfeysi deganda nima tushuniladi?
359. +: kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari
360. -:tashqi qurilmani kompyuterga bog’lashda ishlatiladigan ulovchi simlar
361. -:kompyuterning tashqi portlari.
362. -:tashqi qurilma bilan kompyuter o’rtasida axborot almashinish qoidalari to’plami
363. I:
364. S: Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?
365. +: Yulduz
366. -:Xalqa
367. -:To’liqbog’langan
368. -:Umumiy shina
369. I:
370. S: Ethernet kontsentratori qanday vazifani bajaradi
371. +: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi
372. -:kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo’naltirib beradi
373. -:kompyuterdan kelayotgan axborotni xalqa bo’ylab joylashgan keyingi kompyuterga
374. -:tarmoqning ikki segmentini bir biriga ulaydi
375. I:
376. S: OSI modelida nechta satx mavjud
377. +: 7
378. -:4
379. -:5
380. -:3
381. I:
382. S: OSI modelining to’rtinchi satxi qanday nomlanadi
383. +: Transport satxi
384. -:Amaliy satx
385. -:Seanslar satxi
386. -:Taqdimlash satxi
387. I:
388. S: OSI modelining beshinchi satxi qanday nomlanadi
389. +: Seanslar satxi
390. -:Tarmoq satxi
391. -:Fizik satx
392. -:Amaliy satx
393. I:
394. S: OSI modelining birinchi satxi qanday nomlanadi
395. +: Fizik satx
396. -:Seanslar satxi
397. -:Transport satxi
398. -:Taqdimlash satxi
399. I:
400. S: OSI modelining ikkinchi satxi qanday nomlanadi
401. +: Kanal satxi
402. -:Amaliy satxi
403. -:Fizik satx
404. -:Seanslar satxi
405. I:
406. S: OSI modelining uchinchi satxi qanday nomlanadi
407. +: Tarmoq satxi
408. -:Amaliy satx
409. -:Kanal satxi
410. -:Taqdimlash satxi
411. I:
412. S: OSI modelining oltinchi satxi qanday nomlanadi
413. +: Taqdimlash satxi
414. -:Amaliy satx
415. -:Seanslar satxi
416. -:Kanal satxi
417. I:
418. S: OSI modelining yettinchi satxi qanday nomlanadi
419. +: Amaliy satx
420. -:Seanslar satxi
421. -:Transport satxi
422. -:Taqdimlash satxi
423. I:

S: OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi

1. +: fizik, kanal va tarmoq satxlari
2. -:seans va amaliy satxlar
3. -:amaliy va taqdimlash satxlari
4. -:transport va seans satxlari
5. I:
6. S: OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi
7. +: Marshrutizator
8. -:Ko’prik
9. -:Tarmoq adapter
10. -:Kontsentrator
11. I:
12. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
13. +: Fizik satx
14. -:Kanal satxi
15. -:Tarmoq satxi
16. -:Transport satxi
17. I:
18. S: Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi
19. +: Tarmoq satxi
20. -:Kanal satxi
21. -:Amaliy satx
22. -:Transport satxi
23. I:
24. S: Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub
25. +: IP, IPX
26. -:NFS, FTP
27. -:Ethernet, FDDI
28. -:TCP,UDP
29. I:
30. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
31. +: TCP,UDP
32. -:NFS, FTP
33. -:IP, IPX
34. -:Ethernet, FDDI
35. I:
36. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
37. +: Elektr signallarini uzatish va qabul qilish
38. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojaat qilishni boshqarish
39. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
40. -:Klient dasturlari bilan o’zaro muloqotda bo’lish
41. I:
42. S: Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...
43. +: Avtorizatsiya
44. -:Shifrlash
45. -:Identifikatsiya
46. -:Autentifikatsiya
47. I:
48. S: Autentifikatsiya faktorlari nechta
49. +: 3
50. -:4
51. -:5
52. -: 6
53. I:
54. S: Ko‘z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar?
55. +: Biometrik autentifikatsiya
56. -:Biron nimaga egalik asosida
57. -:Biron nimani bilish asosida
58. -:Parolga asoslangan
59. I:
60. S: Barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi?
61. +: Fizik satx
62. -:Tarmoq satxi
63. -:Amaliy satx
64. -:Tadbiqiy sath
65. I:
66. S: Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi
67. +: 2
68. -:4
69. -:3
70. -:5
71. I:
72. S: Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?
73. +: Subyekt
74. -:Obyekt
75. -:Tizim
76. -:Jarayon
77. I:
78. S: MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi
79. +: xavfsizlik siyosati ma’muri
80. -:Foydalaguvchining o‘zi
81. -:Dastur tomonidan
82. -:Boshqarish amaalga oshirilmaydi
83. I:
84. S: Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi
85. +: O‘qish
86. -:Yozish
87. -:O‘zgartirish
88. -:Yashirish
89. I:
90. S: Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.
91. +: Yozish
92. -:O‘qish
93. -:O‘zgartirish
94. -:Yashirish
95. I:
96. S: Rol tushunchasiga ta’rif bering.
97. +: Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin
98. -:Foydalanishni boshqarish
99. -:Muayyan faoliyat turi bilan bog‘liq imkoniyatlar to‘plami sifatida belgilanishi mumkin
100. -:Vakolitlarni taqsimlash
101. I:
102. S: Foydalanishni boshqarishning qaysi usuli - Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.
103. +: ABAC
104. -:MAC
105. -:DAC
106. -:RBAC
107. I:
108. S: Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?
109. +: barchasi
110. -:bimetrik alomatlarning ishga layoqatli shaxsdan ajratib bo‘lmasligi
111. -:biometrik alomatlarni soxtalashtirishning qiyinligi
112. -:biometrik alomatlarni noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasi yuqoriligi
113. I:
114. S: OSI modeli 7 satxi bu
115. +: Ilova
116. -:Seans
117. -:Fizik
118. -:Kanal
119. I:
120. S: OSI modeli 1 satxi bu
121. +: Fizik
122. -:Ilova
123. -:Seans
124. -:Kanal
125. I:
126. S: OSI modeli 2 satxi bu
127. +:Kanal
128. -: Fizik
129. -:Ilova
130. -:Seans
131. I:
132. S: TCP/IP modelida nechta satx mavjud
133. +: 4
134. -:3
135. -:2
136. -:8
137. I:
138. S: Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi?
139. +: Shaxsiy tarmoq
140. -:Lokal
141. -:Mintaqaviy
142. -:CAMPUS
143. I:
144. S: Tarmoq kartasi bu...
145. +: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
146. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.
147. -:ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
148. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
149. I:
150. S: Server xotirasidagi joyni bepul yoki pulli ijagara berish xizmati qanday ataladi?

1. +: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
2. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
3. -:Signalni tiklash yoki qaytarish uchun foydalaniladi.
4. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
5. I:
6. S: Hab bu...
7. +: ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
8. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
9. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.
10. -:qabul qilingan signalni barchachiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
11. I:
12. S: Tarmoq repiteri bu...
13. +: Signalni tiklash yoki qaytarish uchun foydalaniladi.
14. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
15. -:ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
16. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
17. I:
18. S: Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi.
19. +: DNS tizimlari
20. -:TCP/IP
21. -:Ethernet
22. -:Token ring
23. I:
24. S: ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.
25. +: TCP
26. -:IP
27. -:HTTP
28. -:FTP
29. I:
30. S: …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.
31. +: UDP
32. -:HTTP
33. -:TCP
34. -:FTP
35. I:
36. S: Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi.
37. +: IP
38. -:TCP
39. -:HTTP
40. -:FTP
41. I:
42. S: Tarmoq taxdidlari necha turga bo‘linadi
43. +: 4
44. -:2
45. -:3
46. -:5
47. I:
48. S: Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;
49. +: Razvedka hujumlari
50. -:Kirish hujumlari
51. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
52. -:Zararli hujumlar
53. I:
54. S: Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi
55. +: Kirish hujumlari
56. -:Razvedka hujumlari
57. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
58. -:Zararli hujumlar
59. I:
60. S: Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;
61. +: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
62. -:Razvedka hujumlari
63. -:Kirish hujumlari
64. -:Zararli hujumlar
65. I:
66. S: Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;
67. +: Zararli hujumlar
68. -:Razvedka hujumlari
69. -:Kirish hujumlari
70. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
71. I:
72. S: RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart?
73. +: e soni Eyler funksiyasi - bilan o‘zaro tub
74. -:e ning qiymati [1,n] kesmaga tegishli ixtiyoriy son
75. -:e soni ixtiyoriy tub son
76. -:e soni ixtiyoriy butun musbat son
77. I:
78. S: RSA elektron raqamli imzo algoritmidagi yopiq kalit d qanday hisoblanadi? Bu yerda p va q tub sonlar,n=pq, - Eyler funksiyasi,e-ochiq kalit
79. +:
80. -:
81. -:
82. -:
83. I:
84. S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?
85. +: Imzo qo‘yish va imzoni tekshirishdan
86. -:Faqat imzo qo‘yishdan
87. -:Faqat imzoni tekshirishdan

1. -:Barcha javoblar to‘g‘ri
2. I:
3. S: Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi?
4. +: Imzo muallifining ochiq kaliti yordamida
5. -:Ma’lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida
6. -:Ma’lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida
7. -:Imzo muallifining maxfiy kaliti yordamida
8. I:
9. S: Tarmoq modeli-bu...
10. +: Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir
11. -:Global tarmoq qurish usullari
12. -:Lokal tarmoq qurish usullari
13. -:To‘g‘ri javob yo‘q.
14. I:
15. S: OSI modeli nechta satxga ajraladi?
16. +: 7
17. -:2
18. -:4
19. -:3
20. I:
21. S: TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi
22. +: Kanal, Fizik
23. -:Tarmoq
24. -:Tramsport
25. -:Ilova, taqdimot, seans.
26. I:
27. S: TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi
28. +: Tarmoq
29. -:Kanal, Fizik
30. -:Tramsport
31. -:Ilova, taqdimot, seans.
32. I:
33. S: TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi
34. +: Tramsport
35. -:Kanal, Fizik
36. -:Tarmoq
37. -:Ilova, taqdimot, seans.
38. I:
39. S: TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos keladi
40. +: Ilova, taqdimot, seans
41. -:Kanal, Fizik
42. -:Tarmoq
43. -:Tramsport
44. I:
45. S: Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.
46. +: Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
47. -:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
48. -:Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi
49. -:Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi
50. I:
51. S: Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.
52. +: Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
53. -:Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
54. -:Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi
55. -:Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi.
56. I:
57. S: Repetir nima?
58. +: Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
59. -:Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
60. -: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
61. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
62. I:
63. S: Hub nima?
64. +: Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
65. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi, Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
66. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
67. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
68. I:
69. S: Router nima?
70. +: Qabul qilingan ma’lumotlarni tarmoq satxiga tegishli manzillarga ko‘ra (IP manzil) uzatadi.
71. -:Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
72. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
73. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
74. I:
75. S: Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi
76. +: Razvedka hujumlari
77. -:Kirish hujumlari
78. -:DOS hujumi
79. -:Zararli hujumlar
80. I:
81. S: Razvedka hujumiga berilgan ta’rifni aniqlang
82. +: Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;
83. -:hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi hujumchi -:mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;
84. -:zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;
85. I:
86. S: OSI modelining birinchi satxi qanday nomlanadi
87. +: Fizik satx
88. -:Seanslar satxi
89. -:Transport satxi
90. -:Taqdimlash satxi
91. I:
92. S: OSI modelining ikkinchi satxi qanday nomlanadi
93. +: Kanal satxi
94. -:Amaliy satxi
95. -:Fizik satx
96. -:Seanslar satxi
97. I:
98. S: OSI modelining uchinchi satxi qanday nomlanadi
99. +: Tarmoq satxi
100. -:Amaliy satx
101. -:Kanal satxi
102. -:Taqdimlash satxi
103. I:
104. S: OSI modelining oltinchi satxi qanday nomlanadi
105. +: Taqdimlash satxi
106. -:Amaliy satx
107. -:Seanslar satxi
108. -:Kanal satxi
109. I:
110. S: OSI modelining ettinchi satxi qanday nomlanadi
111. +: Amaliy satx
112. -:Seanslar satxi
113. -:Transport satxi
114. -:Taqdimlash satxi
115. I:
116. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
117. +: Fizik satx
118. -:Kanal satxi
119. -:Tarmoq satxi
120. -:Transport satxi
121. I:
122. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
123. +: TCP,UDP
124. -:NFS, FTP
125. -:IP, IPX
126. -:Ethernet, FDDI
127. I:
128. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
129. +: Elektr signallarini uzatish va qabul qilish
130. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
131. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
132. -:Klient dasturlari bilan o’zaro muloqotda bo’lish
133. I:
134. S: OSI modelining amaliy satxi qanday funksiyalarni bajaradi
135. +: Klient dasturlari bilan o’zaro muloqotda bo’lish
136. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
137. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
138. -:Elektr signallariniuzatish va qabul qilish
139. I:
140. S: Yevklid algoritmi qanday natijani beradi?
141. +: Sonning eng katta umumiy bo’luvchisini toppish
142. -:Sonning turli bo’luvchilarini toppish
143. -:Sonning eng kichik umumiy karralisini toppish
144. -:Sonning eng katta umumiy bo’linuvchisini topish
145. I:
146. S: Qanday sonlar tub sonlar deb yuritiladi?
147. +: Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi.
148. -:O’zidan boshqa bo’luvchilari mavjud bo’lgan sonlar tub sonlar deyiladi.
149. -:Agar sonning 1 dan boshqa bo’luvchilari bo’lsa.
150. -:Faqatgina 1 ga o’ziga bo’linmaydigan sonlar tub sonlar deyiladi.
151. I:
152. S: OSI modelining birinchi satxi qanday nomlanadi
153. +: Fizik satx
154. -:Seanslar satxi
155. -:Transport satxi
156. -:Taqdimlash satxi
157. I:
158. S: OSI modelining ikkinchi satxi qanday nomlanadi
159. +: Kanal satxi
160. -:Amaliy satxi
161. -:Fizik satx
162. -:Seanslar satxi
163. I:
164. S: OSI modelining uchinchi satxi qanday nomlanadi
165. +: Tarmoq satxi
166. -:Amaliy satx
167. -:Kanal satxi
168. -:Taqdimlash satxi
169. I:
170. S: OSI modelining oltinchi satxi qanday nomlanadi
171. +: Taqdimlash satxi
172. -:Amaliy satx
173. -:Seanslar satxi
174. -:Kanal satxi
175. I:
176. S: OSI modelining ettinchi satxi qanday nomlanadi
177. +: Amaliy satx
178. -:Seanslar satxi
179. -:Transport satxi
180. -:Taqdimlash satxi
181. I:
182. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
183. +: Fizik satx
184. -:Kanal satxi
185. -:Tarmoq satxi
186. -:Transport satxi
187. I:
188. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
189. +: TCP,UDP
190. -:NFS, FTP
191. -:IP, IPX
192. -:Ethernet, FDDI
193. I:
194. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
195. +: Elektr signallarini uzatish va qabul qilish
196. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
197. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
198. -:Klient dasturlari bilan o’zaro muloqotda bo’lish
199. I:
200. S: OSI modeliningamaliy satxi qanday funktsiyalarni bajaradi
201. +: Klient dasturlari bilan o’zaro muloqotda bo’lish
202. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
203. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
204. -:Elektr signallariniuzatish va qabul qilish
205. I:
206. S: Yevklid algoritmi qanday natijani beradi?
207. +: Sonning eng katta umumiy bo’luvchisini toppish
208. -:Sonning turli bo’luvchilarini toppish
209. -:Sonning eng kichik umumiy karralisini toppish
210. -:Sonning eng katta umumiy bo’linuvchisini topish
211. I:
212. S: Qanday sonlar tub sonlar deb yuritiladi?
213. +: Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi.
214. -:O’zidan boshqa bo’luvchilari mavjud bo’lgan sonlar tub sonlar deyiladi.
215. -:Agar sonning 1 dan boshqa bo’luvchilari bo’lsa.
216. -:Faqatgina 1 ga o’ziga bo’linmaydigan sonlar tub sonlar deyiladi.
217. I:
218. S: Antivirus dasturlarini ko’rsating?
219. +: Drweb, Nod32, Kaspersky
220. -:arj, rar, pkzip, pkunzip
221. -:winrar, winzip, winarj
222. -:pak, lha
223. I:
224. S: Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi
225. +: wep, wpa, wpa2
226. -:web, wpa, wpa2
227. -:wpa, wpa2
228. -:wpa, wpa2, wap
229. I:
230. S: Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak?
231. +: ishonchli, qimmatli va to’liq
232. -:uzluksiz va uzlukli
233. -:ishonchli, qimmatli va uzlukli
234. -:ishonchli, qimmatli va uzluksiz
235. I:
236. S: Axborotning eng kichik o’lchov birligi nima?
237. +: bit
238. -:kilobayt
239. -:bayt
240. -:bitta simvol
241. I:
242. S: Virtual xususiy tarmoq – bu?
243. +: VPN
244. -:APN
245. -:ATM
246. -:Ad-hoc
247. I:
248. S: Xavfli viruslar bu - …
249. +: kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar
250. -:tizimda mavjudligi turli taassurot (ovoz, video) bilan bog’liq viruslar, bo’sh xotirani kamaytirsada, dastur va ma`lumotlarga ziyon yetkazmaydi
251. -:o’z-o’zidan tarqalish mexanizmi amalga oshiriluvchi viruslar
252. -:dastur va ma`lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o’chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar
253. I:
254. S: Mantiqiy bomba – bu …
255. +: Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari
256. -:Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari
257. -:Viruslar kodiga boshqarishni uzatish
258. -:Qidirishning passiv mexanizmlarini amalga oshiruvchi, yahni dasturiy fayllarga tuzoq qo’yuvchi viruslar
259. I:
260. S: Rezident virus...
261. +: tezkor xotirada saqlanadi
262. -:to’liqligicha bajarilayotgan faylda joylashadi
263. -:ixtiyoriy sektorlarda joylashgan bo’ladi
264. -:alohida joyda joylashadi
265. I:
266. S: DIR viruslari nimani zararlaydi?
267. +: FAT tarkibini zararlaydi
268. -:com, exe kabi turli fayllarni zararlaydi
269. -:yuklovchi dasturlarni zararlaydi
270. -:Operatsion tizimdagi sonfig.sys faylni zararlaydi
271. I:
272. S:.... kompyuter tarmoqlari bo’yicha tarqalib, komlg’yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi
273. +: «Chuvalchang» va replikatorli virus
274. -:Kvazivirus va troyan virus
275. -:Troyan dasturi
276. -:Mantiqiy bomba
277. I:
278. S: Fire Wall ning vazifasi...
279. +: tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi
280. -:kompyuterlar tizimi xavfsizligini ta`minlaydi
281. -:Ikkita kompyuter o’rtasida aloqa o’rnatish jarayonida Internet tarmog’i orasida xavfsizlikni ta`minlaydi
282. -:uy tarmog’i orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi
283. I:
284. S: Kompyuter virusi nima?
285. +: maxsus yozilgan va zararli dastur
286. -:.exe fayl
287. -:boshqariluvchi dastur
288. -:Kengaytmaga ega bo’lgan fayl
289. I:
290. S: Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating
291. +: disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali
292. -: faqat maxsus tashuvchi qurilma orqali
293. -: faqat kompyuter tarmoqlari orqali
294. -:zararlanish yo’llari juda ko’p
295. I:
296. S: Troyan dasturlari bu...
297. +: virus dasturlar
298. -:antivirus dasturlar
299. -:o’yin dasturlari
300. -:yangilovchi dasturlar
301. I:
302. S: Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi?
303. +: 5
304. -:4
305. -:2
306. -:3
307. I:
308. S: Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud
309. +: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar
310. -:detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar
311. -:vaktsinalar, privivkalar, revizorlar, tekshiruvchilar
312. -:privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar
313. I:
314. S: Stenografiya mahnosi...
315. +: sirli yozuv
316. -:sirli xat
317. -:maxfiy axborot
318. -:maxfiy belgi
319. I:
320. S: …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi
321. +: K.Shennon
322. -:Sezar
323. -:U.Xill
324. -:Fon Neyman
325. I:
326. S: Kriptologiya yo’nalishlari nechta?
327. +: 2
328. -:3
329. -:4
330. -:5
331. I:
332. S: Kriptografiyaning asosiy maqsadi...
333. +: maxfiylik, yaxlitlilikni ta`minlash
334. -:ishonchlilik, butunlilikni ta`minlash
335. -:autentifikatsiya, identifikatsiya
336. -:ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya
337. I:
338. S: DES algoritmi akslantirishlari raundlari soni qancha?
339. +: 16;
340. -:14;
341. -:12;
342. -:32;
343. I:
344. S: DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha?
345. +: CHap qism blok 32 bit, o‘ng qism blok 32 bit;
346. -:CHap qism blok 32 bit, o‘ng qism blok 48 bit;
347. -:CHap qism blok 64 bit, o‘ng qism blok 64 bit;
348. -:CHap qism blok 16 bit, o‘ng qism blok 16 bit;
349. I:
350. S: 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta?
351. +: 18 ta;
352. -:19 ta
353. -:11 ta
354. -:9 ta
355. I:
356. S: 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta?
357. +: 3 ta
358. -:7 ta
359. -:8 ta;
360. -:9 ta
361. I:
362. S: Qaysi formula qoldiqli bo’lish qonunini ifodalaydi
363. +: a = *bq + r,* ,
364. -:
365. -:M=r1^k2;
366. -:M=
367. I:
368. S: Eyler funksiyasida p=11 va q=13 sonining qiymatini toping.
369. +: 16
370. -:59
371. -:30
372. -:21
373. I:
374. S: Eyler funksiyasi yordamida 1811 sonining qiymatini toping.
375. +: 1810
376. -:2111
377. -:16
378. -:524
379. I:
380. S: 97 tub sonmi?
381. +: Tub
382. -:murakkab
383. -:Natural
384. -:To’g’ri javob yo’q
385. I:
386. S: Quyidagi modulli ifodani qiymatini toping
387. (148 + 14432) mod 256.
388. +: 244
389. -:200
390. -:156
391. -:154
392. I:
393. S: Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220
394. +: 44
395. -:21
396. -:42
397. -:20
398. I:
399. S: Quyidagi ifodani qiymatini toping. -16mod11
400. +: 6
401. -:5
402. -:7
403. -:11
404. I:
405. S: 2 soniga 10 modul bo’yicha teskari sonni toping.
406. +: Ø
407. -:3
408. -:10
409. -:25
410. I:
411. S: 2 soniga 10 modul bo’yicha teskari sonni toping.
412. +: Ø
413. -:3
414. -:10
415. -:25
416. I:
417. S: DES da dastlabki kalit uzunligi necha bitga teng?
418. +:56 bit
419. -:128 bit
420. -:64 bit
421. -:32 bit
422. I:
423. S: DES da bloklar har birining uzunligi necha bitga teng?
424. +:32 bit
425. -:56 bit
426. -:48 bit
427. -:64 bit
428. I:
429. S: DES da raundlar soni nechta?
430. +:16
431. -:32
432. -:8
433. -:48
434. I:
435. S: Shifrlash kaliti noma’lum bo’lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi
436. +:kriptobardoshlik
437. -:Shifr matn uzunligi
438. -:Shifrlash algoritmi
439. -:Texnika va texnologiyalar
440. I:
441. S: Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo’linadi
442. +:blokli va oqimli
443. -:DES va oqimli
444. -:Feystel va Verman
445. -:SP− tarmoq va IP
446. I:
447. S: DES shifrlash algoritmida shifrlanadigan malumotlar bloki necha bit?
448. +:64
449. -:32
450. -:48
451. -:56
452. I:
453. S: XOR amali qanday amal?
454. +:2 modul bo`yicha qo`shish
455. -:264 modul bo`yicha qo`shish
456. -:232 modul bo`yicha qo`shish
457. -:248 modul bo`yicha qo`shish
458. I:
459. S: 4+31 mod 32 ?
460. +:3
461. -:4
462. -:31
463. -:32
464. I:
465. S: 21+20mod32?
466. +:9
467. -:12
468. -:16
469. -:41
470. I:
471. S: 12+22 mod 32 ?
472. +:2
473. -:12
474. -:22
475. -:32
476. I:
477. S: AES algoritmi bloki uzunligi … bitdan kam bo’lmasligi kerak.
478. +:128
479. -:512
480. -:256
481. -:192
482. I:
483. S: Xesh-:funktsiyani natijasi …
484. +:fiksirlangan uzunlikdagi xabar
485. -:Kiruvchi xabar uzunligidagi xabar
486. -:Kiruvchi xabar uzunligidan uzun xabar
487. -:fiksirlanmagan uzunlikdagi xabar
488. I:
489. S: 2+5 mod32 ?
490. +:7
491. -:32
492. -:2
493. -:5
494. I:
495. S: 97 tub sonmi?
496. +:Tub
497. -:murakkab
498. -:Natural
499. -:To’g’ri javob yo’q
500. I:
501. S: Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing.
502. +:23
503. -:20
504. -:21
505. -:19
506. I:
507. S: Quyidagi ifodani qiymatini toping. -17mod11
508. +:5
509. -:6
510. -:7
511. -:11
512. I:
513. S: Diskni shifrlash nima uchun amalga oshiriladi?
514. +: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
515. -:Xabarni yashirish uchun amalga oshiriladi
516. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi
517. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi
518. I:
519. S: Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?
520. +: 4
521. -:8
522. -:7
523. -:5
524. I:
525. S: OSI modelida nechta tarmoq satxi bor
526. +: 7
527. -:6
528. -:5
529. -:4
530. I:
531. S: Diskni shifrlash nima uchun amalga oshiriladi?
532. +: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
533. -:Xabarni yashirish uchun amalga oshiriladi
534. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi
535. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi
536. I:
537. S: Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?
538. +: 4
539. -:8
540. -:7
541. -:5
542. I:
543. S: OSI modelida nechta tarmoq satxi bor
544. +: 7
545. -:6
546. -:5
547. -:4
548. I:
549. S: “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonun moddadan iborat
550. +:16
551. -:18
552. -:11
553. -:14
554. I:
555. S: Kompyuter etikasi instituti notijoriy tashkilot tomonidan texnologiyani axloqiy nuqta nazardan targ‘ib qilish bo‘yicha nechta etika qoidalari keltirilgan
556. +:10
557. -:18
558. -:11
559. -:14
560. I:
561. S: Kiberjinoyatchilik bu –. . .
562. +: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.
563. -: Kompyuter o‘yinlari
564. -: Faqat banklardan pul o‘g‘irlanishi
565. -: autentifikatsiya jarayonini buzish
566. I:
567. S: Fishing nima?
568. +: Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.
569. -: Ma’lumotlar bazalarini xatoligi
570. -: Mualliflik huquqini buzilishi
571. -: Lug‘at orqali xujum qilish.
572. I:
573. S: Bag nima?
574. +: Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo
575. -: Mualliflik huquqini buzilishi
576. -: Dasturlardagi ortiqcha reklamalar
577. -: Autentifikatsiya jarayonini buzish
578. I:
579. S: Nuqson nima?
580. +: Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi nuqsondir
581. -: Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo
582. -: Dasturlardagi ortiqcha reklamalar
583. -: Autentifikatsiya jarayonini buzish
584. I:
585. S: Quyidagilardan qaysi birida xavfsiz dasturlash tillari keltirilgan.
586. +: C#, Scala, Java
587. -: C, C#, java
588. -: C++, Scala, Java
589. -: Misra-C, Java, c++
590. I:
591. S: Quyidagilardan qaysi biri dasturiy maxsulotlarga qo‘yiladigan xavfsizlik talablari hisoblanidi.
592. +: Vazifaviy, novazifaviy, qolgan talablar
593. -: Qolgan talablar, anaviy taablar, etika talablari
594. -: Vazifaviy, novazifaviy, etika talablari.
595. -: Vazifaviy, etika talablari, foydalanuvchanlik talablari.
596. I:
597. S: Dasturiy ta’minotda kirish va chiqishga aloqador bo‘lgan talablar qanday talablar sirasiga kiradi?
598. +:Vazifaviy
599. -: Novazifaviy
600. -: Etika talablari
601. -: Qolgan talablar
602. I:
603. S: Dasturda tizim amalga oshirishi kerak bo‘lgan vazifalar bu..
604. +:Vazifaviy
605. -: Novazifaviy
606. -: Etika talablari
607. -: Qolgan talablar
608. I:
609. S: Risklarni boshqarishda risklarni aniqlash jarayoni bu-..
610. +: Tashkilot xavfsizligiga ta’sir qiluvchi tashqi va ichki risklarning manbasi, sababi, oqibati va haklarni aniqlash.
611. -: Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta’siri va ehtimolini o‘lchashni ta’minlaydi.
612. -: Risklarni davolash bu – aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni.
613. -: Risk monitoringi yangi risklarni paydo bo‘lish imkoniyatini aniqlash.
614. I:
615. S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.
616. +:"Sovuq saxiralash"
617. -:"Issiq zaxiralash"
618. -:"Iliq saxiralash"
619. -:"To'liq zaxiralash"
620. I:
621. S: Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishi bilan bog'liq bo'lsa bu nima deb yuritiladi?
622. +:Jinoyat sifatida baholanadi
623. -:Rag’bat hisoblanadi
624. -:Buzgunchilik hisoblanadi
625. -:Guruhlar kurashi hisoblanadi
626. I:
627. S: Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun qanday kalit ishlatiladi?
628. +:Ikkita kalit
629. -:Bitta kalit
630. -:Elektron raqamli imzo
631. -:Foydalanuvchi identifikatori
632. I:
633. S:Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?
634. +:Axborot xavfsizligi buzulgan taqdirda ko’rilishi mumkin bo’lgan zarar miqdori bilan
635. -:Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhumligi bilan
636. -:Axborotni noqonuniy foydalanishlardan o’zgartirishlardan va yo’q qilishlardan himoyalanganligi bilan
637. -:Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bilan}
638. I:
639. S:Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?
640. +:Strukturalarni ruxsatsiz modifikatsiyalash
641. -:Tabiy ofat va avariya
642. -:Texnik vositalarning buzilishi va ishlamasligi
643. -:Foydalanuvchilar va xizmat ko‘rsatuvchi hodimlarning hatoliklari}
644. I:
645. S:Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?
646. +:Texnik vositalarning buzilishi va ishlamasligi
647. -:Axborotdan ruhsatsiz foydalanish
648. -:Zararkunanda dasturlar
649. -:An’anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili}
650. I:
651. S:Axborot xavfsizligini ta'minlovchi choralarni ko’rsating?
652. +:1-huquqiy, 2-tashkiliy-ma'muriy, 3-injener-texnik
653. -:1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy
654. -:1-dasturiy, 2-tashkiliy-ma'muriy, 3-huquqiy
655. -:1-aparat, 2-texnikaviy, 3-huquqiy}
656. I:
657. S:Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o’z ichiga oladi
658. +:Xalqaro va milliy huquqiy me’yorlarni
659. -:Tashkiliy va xalqaro me’yorlarni
660. -:Ananaviy va korporativ me’yorlarni
661. -:Davlat va nodavlat tashkilotlarime’yorlarni}
662. I:
663. S:Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?
664. +: Ma’lumotlar butunligi
665. -:Axborotning konfedensialligi
666. -:Foydalanuvchanligi
667. -:Ixchamligi}

1. I:
2. S:Axborotning buzilishi yoki yo‘qotilishi xavfiga olib keluvchi himoyalanuvchi ob’ektga qarshi qilingan xarakatlar qanday nomlanadi?
3. +:Tahdid
4. -:Zaiflik
5. -:Hujum
6. -:Butunlik}
7. I:
8. S:Biometrik autentifikatsiyalashning avfzalliklari-bu:
9. +:Biometrik alomatlarning noyobligi
10. -:Bir marta ishlatilishi
11. -:Biometrik alomatlarni o’zgartirish imkoniyati
12. -:Autentifikatsiyalash jarayonining soddaligi
13. I:
14. S: Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari-bu:
15. +:Foydalanuvchanligi
16. -:Ma’lumotlar butunligi
17. -:Axborotning konfedensialligi
18. -:Ixchamligi
19. I:
20. S:Global simsiz tarmoqning ta`sir doirasi qanday?
21. +:Butun dunyo bo’yicha
22. -:Binolar va korpuslar
23. -:O’rtacha kattalikdagishahar
24. -:Foydalanuvchi yaqinidagi tarmoq
25. I:
26. S: Foydalanuvchini identifikatsiyalashda qanday ma’lumotdan foydalaniladi?
27. +:Identifikatori
28. -:Telefon raqami
29. -:Parol
30. -:Avtorizatsiyasi
31. I:
32. S: Foydalanuvchining tarmoqdagi harakatlarini va resurslardan foydalanishga urinishini qayd etish-bu:
33. +:Ma`murlash
34. -:Autentifikatsiya
35. -:Identifikatsiya
36. -:Sertifikatsiyalash
37. I:
38. S: Kompyuter tizimini ruxsatsiz foydalanishdan himoyalashni, muhim kompyuter tizimlarni rezervlash, o‘g‘irlash va diversiyadan himoyalanishni ta’minlash rezerv elektr manbai, xavfsizlikning maxsus dasturiy va apparat vositalarini ishlab chiqish va amalga oshirish qaysi choralarga kiradi?
39. +:Injener-texnik
40. -:Molyaviy
41. -:Tashkiliy-ma’muriy
42. -:Huquqiy
43. I:
44. S: Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi-bu:
45. +:Autentifikatsiya
46. -:Identifikatsiya
47. -:Ma`murlash (accaunting)
48. -:Avtorizatsiya
49. I:
50. S: O‘zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi–bu:
51. +:Tarmoq viruslari
52. -:Pochta viruslari
53. -:Fayl viruslari
54. -:Protokol viruslari
55. I:
56. S: Qanday viruslar xavfli hisoblanadi?
57. +:kompyuter ishlashida jiddiy nuqsonlarga olib keluvchi
58. -:Jiddiy nuqsonlarga olib kelmaydigan ammo foydalanuvchini chalg'itadigan.
59. -:Katta viruslar va odatda zararli dasturlar
60. -:Passiv viruslar
61. I:
62. S: Rezident bo’lmagan viruslar qachon xotirani zararlaydi?
63. +:Faqat faollashgan vaqtida
64. -:Faqat o’chirilganda
65. -:Kompyuter yoqilganda
66. -:Tarmoq orqali ma’lumot almashishda
67. I:
68. S: Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan iborat?
69. +:Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud
70. -:Tarmoq chetki nuqtalari orasidagi xududning kengligi asosida qurilmalarholati
71. -:Himoya vositalarining chegaralanganligi
72. -:Himoyani amalga oshirish imkoniyati yo‘qligi va ma'lum protokollarning ishlatilishi
73. I:
74. S: Simmetrik shifrlashning noqulayligi – bu:
75. +:Maxfiy kalitlar bilan ayirboshlash zaruriyatidir
76. -:Kalitlar maxfiyligi
77. -:Kalitlar uzunligi
78. -:SHifrlashga ko‘p vaqt sarflanishi va ko'p yuklanishi
79. I:
80. S: Simsiz tarmoqlarni kategoriyalarini to’g’ri ko’rsating?
81. +:Simsiz shaxsiy tarmoq (PAN), simsiz lokal tarmoq (LAN), simsiz regional tarmoq (MAN) va Simsiz global tarmoq (WAN)
82. -:Simsiz internet tarmoq (IAN )va Simsiz telefon tarmoq (WLAN), Simsiz shaxsiy tarmoq (PAN) va Simsiz global tarmoq (WIMAX)
83. -:Simsiz internet tarmoq (IAN) va uy simsiz tarmog’i
84. -:Simsiz chegaralanmagan tarmoq (LAN), simsiz kirish nuqtalari

1. I:
2. S: Sub`ektga ma`lum vakolat va resurslarni berish muolajasi-bu:
3. +:Avtorizatsiya
4. -:Haqiqiylikni tasdiqlash
5. -:Autentifikatsiya
6. -:Identifikasiya

I:

1. S: Tarmoq operatsion tizimining to'g'ri konfiguratsiyasini madadlash masalasini odatda kim hal etadi?
2. +:Tizim ma'muri
3. -:Tizim foydalanuvchisi
4. -:Korxona raxbari
5. -:Operator
6. I:
7. S: Tarmoqlararo ekran texnologiyasi-bu:
8. +:Ichki va tashqi tarmoq o’rtasida filtr va himoya vazifasini bajaradi
9. -:Ichki va tashqi tarmoq o’rtasida axborotni o’zgartirish vazifasini bajaradi
10. -:Qonuniy foydalanuvchilarni himoyalash
11. -:Ishonchsiz tarmoqdan kirishni boshqarish}
12. I:
13. S: Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko’rsating?
14. +:DDoS (Distributed Denial of Service) hujum
15. -:Tarmoq hujumlari
16. -:Dastur hujumlari asosidagi (Denial of Service) hujum
17. -:Virus hujumlari}
18. I:
19. S: Uyishtirilmagan tahdid, ya’ni tizim yoki dasturdagi qurilmaning jismoniy xatoligi – bu…
20. +:Tasodifiy tahdid
21. -:Uyishtirilgan tahdid
22. -:Faol tahdid
23. -:Passiv tahdid
24. I:
25. S: Axborot xavfsizligi qanday asosiy xarakteristikalarga ega?
26. +:Butunlik, konfidentsiallik, foydalana olishlik
27. -:Butunlik, himoya, ishonchlilikni urganib chiqishlilik
28. -:Konfidentsiallik, foydalana olishlik
29. -:Himoyalanganlik, ishonchlilik, butunlik
30. }
31. I:
32. S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.
33. +:"Sovuq saxiralash"
34. -:"Issiq zaxiralash"
35. -:"Iliq saxiralash"
36. -:"To'liq zaxiralash"
37. I:
38. S: Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?
39. +:"Issiq zaxiralash"
40. -:"Sovuq saxiralash"
41. -:"Iliq saxiralash"
42. -:"To'liq zaxiralash"
43. I:
44. S: Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang
45. +:HandyBakcup
46. -:Recuva, R.saver
47. -:Cryptool
48. -:Eset32
49. I:
50. S: O'chirilgan, formatlangan ma'lumotlarni tikovchi dasturni belgilang.
51. +:Recuva, R.saver
52. -:HandyBakcup
53. -:Cryptool
54. -:Eset32
55. I:
56. S: Virtuallashtirishga qaratilgan dasturiy vositalarni belgilang.
57. +:VMware, VirtualBox
58. -:HandyBakcup
59. -:Eset32
60. -:Cryptool
61. I:
62. S: Cloud Computing texnologiyasi nechta katta turga ajratiladi?
63. +:3 turga
64. -:2 turga
65. -:4 turga
66. -:5 turga
67. I:
68. S: O'rnatilgan tizimlar-bu…
69. +:Bu ko'pincha real vaqt hisoblash cheklovlariga ega bo'lgan kattaroq mexanik yoki elektr tizimidagi maxsus funksiyaga ega, boshqaruvchidir
70. -:Korxona ichki tarmog’iga ulangan korporativ tarmog’idan bo'ladigan hujumlardan himoyalash
71. -:Korxona ichki tarmog’ini Internet global tarmog’idan ajratib qo’yish
72. -:Bu ko'pincha global tizimda hisoblash cheklovlariga ega bo'lgan mexanik yoki elektr tizimidagi maxsus funksiyaga ega qurilmadir
73. I:
74. S: Axborotdan oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan?
75. +:AQSH sog'liqni saqlash va insonlarga xizmat ko'rsatish vazirligi
76. -:AQSH Mudofaa vazirligi
77. -:O'zbekiston Axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi
78. -:Rossiya kiberjinoyatlarga qarshu kurashish davlat qo'mitasi
79. I:
80. S: Axborotdan oqilona foydalanish kodeksi nechanchi yil ishlab chiqilgan?
81. +:1973 yil
82. -:1980 yil
83. -:1991 yil
84. -:2002 yil
85. I:
86. S: Kompyuter bilan bog'liq falsafiy soha bo'lib, foydalanuvchilarning xatti-harakatlari, komyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko'rsatishini o'rgatadigan soha nima deb ataladi?
87. +:Kiberetika
88. -:Kiberhuquq
89. -:Kiberqoida
90. -:Kiberxavfsizlik
91. I:
92. S: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…
93. +:Kiberjinoyat
94. -:Kibersport
95. -:Kiberterror
96. -:Hakerlar uyushmasi
97. I:
98. S: Tarmoqlararo ekran paket filtrlari qaysi sathda ishlaydi?
99. +:Tarmoq sathida
100. -:Ilova sathida
101. -:Kanal sathida
102. -:Fizik sathida
103. I:
104. S: Tarmoqlararo ekran ekspert paketi filtrlari qaysi sathda ishlaydi?
105. +:Transport sathida
106. -:Ilova sathida
107. -:Kanal sathida
108. -:Fizik sathida
109. I:
110. S: Spam bilan kurashishning dasturiy uslubida nimalar ko’zda tutiladi?
111. +:Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida filtrlanib cheklanadi
112. -:Elektron pochta qutisiga kelib tushadigan spamlar me’yoriy xujjatlar asosida cheklanadi va bloklanadi
113. -:Elektron pochta qutisiga kelib tushadigan spamlar ommaviy ravishda cheklanadi
114. -:Elektron pochta qutisiga kelib spamlar mintaqaviy hududlarda cheklanadi
115. I:
116. S: Ma’lumotlarni yo’qolish sabab bo’luvchi tabiiy tahdidlarni ko’rsating
117. +:Zilzila, yong‘in, suv toshqini va hak
118. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
119. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
120. -:Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani
121. I:
122. S: Ma’lumotlarni tasodifiy sabablar tufayli yo’qolish sababini belgilang
123. +:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
124. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
125. -:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
126. -:Zilzila, yong‘in, suv toshqini va hak
127. I:
128. S: Ma’lumotlarni inson xatosi tufayli yo’qolish sababini belgilang.
129. +:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
130. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
131. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
132. -:Zilzila, yong‘in, suv toshqini va hak
133. I:
134. S: Ma’lumotlarni g’arazli hatti harakatlar yo’qolish sababini ko’rsating.
135. +:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
136. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
137. -:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
138. -:Zilzila, yong‘in, suv toshqini va hak
139. I:
140. S: Kompyuterda hodisalar haqidagi ma’lumot qayerda saqlanadi?
141. +:Hodisalar jurnaliga
142. -:Operativ xotiraga
143. -:Kesh xotiraga
144. -:Vaqtinchalik faylga
145. I:
146. S: Internet orqali masofada joylashgan kompyuterga yoki tarmoq resurslariga DoS hujumlari uyushtirilishi natijasida..
147. +:Foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan mahrum qilinadilar
148. -:Foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzg’unchilarga etkaziladi
149. -:Axborot tizimidagi ma’lumotlar bazalari o’g’irlanib ko’lga kiritilgach, ular yo’q qilinadilar
150. -:Foydalanuvchilar axborotlariga ruxsatsiz o’zgartirishlar kiritilib, ularning yaxlitligi buziladi
151. I:
152. S: Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo’naltirilgan buzg’unchi bu - ... .
153. +:Krakker
154. -:Hakker
155. -:Virus bot
156. -:Ishonchsiz dasturchi
157. I:
158. S: Antivirus dasturiy vositalari viruslarni tahlil qilishiga ko'ra necha turga bo'linadi?
159. +:2 turga: fayl Signaturaga va evristikaga asoslangan
160. -:2 turga: faol va passiv
161. -:2 turga: pulli va pulsiz
162. -:2 turga: litsenziyali va ochiq
163. I:
164. S: "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?
165. +:Foydalanish davrida maxfiylik kamayib boradi
166. -:Parolni esda saqlash kerak bo'ladi
167. -:Parolni almashtirish jarayoni murakkabligi
168. -:Parol uzunligi soni cheklangan
169. I:
170. S: Yaxlitlikni buzilishi bu - …
171. +:Soxtalashtirish va o’zgartirish
172. -:Ishonchsizlik va soxtalashtirish
173. -:Soxtalashtirish
174. -:Butunmaslik va yaxlitlanmaganlik
175. I:
176. S: Tarmoqda joylashgan fayllar va boshqa resurslardan foydalanishni taqdim etuvchi tarmoqdagi kompyuter nima?
177. +:Server
178. -:Bulutli tizim
179. -:Superkompyuter
180. -:Tarmoq
181. I:
182. S: Tahdid nima?
183. +:Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.
184. -:Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa
185. -:Bu riskni o‘zgartiradigan harakatlar bo‘lib
186. -:Bu noaniqlikning maqsadlarga ta’siri
187. I:
188. S: Risk nima?
189. +:Potensial kuchlanish yoki zarar
190. -:Potensial foyda yoki zarar
191. -:Tasodifiy taxdid
192. -:Katta yo‘qotish
193. I:
194. S: Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi?
195. +:Optik tolali
196. -:O’rama juft
197. -:Koaksial
198. -:Telefon kabeli
199. I:
200. S: Nima uchun autentifikatsiyalashda parol ko’p qo’llaniladi?
201. +:Sarf xarajati kam, almashtirish oson
202. -:Parolni eslab qolish oson
203. -:Parolni o’g’rishlash qiyin
204. -:Serverda parollarni saqlash oson
205. I:
206. S: Elektron xujjatlarni yo’q qilish usullari qaysilar?
207. +:Shredirlash, magnitsizlantirish, yanchish
208. -:Yoqish, ko’mish, yanchish
209. -:Shredirlash, yoqish, ko’mish
210. -:Kimyoviy usul, yoqish.
211. I:
212. S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?
213. +:Imzo qo‘yish va imzoni tekshirishdan
214. -:Faqat imzo qo‘yishdan
215. -:Faqat imzoni tekshirishdan
216. -:Kalitlarni taqsimlashdan
217. I:
218. S: Elektron pochtaga kirishda foydalanuvchi qanday autetntifikasiyalashdan o’tadi?
219. +:Parol asosida
220. -:Smart karta asosida
221. -:Biometrik asosida
222. -:Ikki tomonlama
223. I:
224. S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Jazolar bosqichiga to‘g‘ri ta’rif berilgan.
225. -: tashkilot o‘z siyosatini ishlab chiqishdan oldin o‘z aktivlari uchun risklarni baholashi shart
226. -: tashkilot o‘z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o‘rnatilish shart
227. -: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo‘shimcha kiritish jarayonida boshqaruvchi bo‘lishi shart
228. +: ma’lum tashkilotlarda tashkilotlarda qat’iy siyosatlar mavjud. Agar xodimlar ushbu siyosatlarga amal qilmasa, ularga qarshi bir qancha choralar qo‘llaniladi.
229. I:
230. S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Xodimlarni o‘rgatish bosqichiga to‘g‘ri ta’rif berilgan.
231. -: tashkilot o‘z siyosatini ishlab chiqishdan oldin o‘z aktivlari uchun risklarni baholashi shart
232. -: tashkilot o‘z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o‘rnatilish shart
233. -: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo‘shimcha kiritish jarayonida boshqaruvchi bo‘lishi shart
234. +: xodimlarga tashkilot xavfsizlik siyosati davomli ravishda o‘rgatilishi shart
235. I:
236. S: Galstuk babochka usuli nima?
237. +: Risklarni baholash usuli
238. -: Risklarni qabul qilish usuli
239. -: shifrlash algoritmi
240. -: Risklarni hosil qilish usuli.
241. I:
242. S: Lotin alifbosida DADA so‘zini 3 kalit bilan shifrlagandan so‘ng qaysi so‘z hosil bo‘ladi. A=0, B=1….Z=25.
243. +:GDGD
244. -: NANA
245. -: GPGP
246. -: FDFD
247. I:
248. S: Lotin alifbosida NON so‘zini 3 kalit bilan shifrlagandan so‘ng qaysi so‘z hosil bo‘ladi. A=0, B=1….Z=25.
249. -:GDGD
250. -: NANA
251. +: QRQ
252. -: FDFD
253. I:
254. S: Fizik to‘siqlarni o‘rnatish , Xavfsizlik qo‘riqchilarini ishga olish, Fizik qulflar qo‘yishni amalga oshirish qanday nazorat turiga kiradi?
255. +:Fizik nazorat
256. -: Texnik nazorat
257. -: Ma’muriy nazorat
258. -: Tashkiliy nazorat
259. I:
260. S: Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?
261. -: Fizik nazorat
262. +:Texnik nazorat
263. -: Ma’muriy nazorat
264. -: Tashkiliy nazorat
265. I:
266. S: Qoida va muolajalarni yaratish, Joylashuv arxitekturasini loyihalash, Xavfsizlik belgilari va ogohlantirish signallari, Ishchi joy xavfsizligini ta’minlash, Shaxs xavfsizligini ta’minlash amalga oshirish qanday nazorat turiga kiradi?
267. -: Fizik nazorat
268. -: Texnik nazorat
269. +: Ma’muriy nazorat
270. -: Tashkiliy nazorat
271. I:
272. S: Ikkilik sanoq tizimida qanday raqamlardan foydalanamiz?
273. +: Faqat 0 va 1
274. -: Faqat 1
275. -: Faqat 0
276. -: Barcha raqamlardan
277. I:
278. S: AES shifrlash algoritmi necha rounddan iborat
279. +: 10, 12, 14
280. -: 10,14,16
281. -: 12,14,16
282. -: 16
283. I:
284. S: Hodisalar daraxti usuli nima?
285. +: Risklarni baholash usuli
286. -: Risklarni qabul qilish usuli
287. -: shifrlash algoritmi
288. -: Risklarni hosil qilish usuli
289. I:
290. S: Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?
291. +:3 taga
292. -:4 taga
293. -:2 taga
294. -:5 taga

1. I:
2. S: WiMAX qanday simsiz tarmoq turiga kiradi.
3. +: Regional
4. -: Lokal
5. -: Global
6. -: Shaxsiy
7. I:
8. S: Wi-Fi necha Gs chastotali to'lqinda ishlaydi?
9. +: 2.4-5 Gs
10. -: 2.4-2.485 Gs
11. -: 1.5-11 Gs
12. -: 2.3-13.6 Gs
13. I:
14. S: Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi?
15. +: Onx458&hdsh)
16. +: 12456578
17. +: salomDunyo
18. +: Mashina777
19. I:
20. S: Parollash siyosatiga ko'ra parol tanlash shartlari qanday?
21. +: Kamida 8 belgi: katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. -: Kamida 8 belgi: katta va kichik xavflar, sonlar qo'llanishi kerak.
22. -: Kamida 6 belgi: katta xarflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak.
23. -: Kamida 6 belgi: katta va kichik xarflar, kamida bitta maxsus simvol qo'llanishi kerak.

1. Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

Foydalanishni boshqarish   
2. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?   
Xalqa   
3. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?   
Biometrik autentifikatsiya   
5. Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?   
Texnik nazorat   
6. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating   
Zilzila, yong‘in, suv toshqini va hak.   
7. Token, Smartkartalarda xavfsizlik tomonidan kamchiligi nimada?   
Qurilmalarni ishlab chiqarish murakkab jarayon   
8. Foydalanishni boshqarish –bu...   
Sub’ektni Sub’ektga ishlash qobilyatini aniqlashdir.   
9. Ro‘yxatdan o‘tish-bu…   
foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni   
10. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?   
Xavfsizlik siyosati ma’muri   
11. MD5, SHA1, SHA256, O‘z DSt 1106:2009- qanday algoritmlar deb ataladi?   
Shifrlash   
12. Shifr nima?   
Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm   
13. Ethernet kontsentratori qanday vazifani bajaradi?   
kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo‘naltirib beradi   
14. Tekstni boshqa tekst ichida ma’nosini yashirib keltirish nima deb ataladi?   
steganografiya   
15. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?   
{d, n} – yopiq, {e, n} – ochiq;   
16. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?   
1-2 jahon urushu davri   
17. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?   
Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi   
18. ……–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.   
Kiberxavfsizlik   
19. Kriptografiyaning asosiy maqsadi nima?   
maxfiylik, yaxlitlilikni ta’minlash   
20. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.   
ABAC

### 1. Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

 Foydalanishni boshqarish

### 2. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?

 Xalqa

### 3. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

 Biometrik autentifikatsiya

### 5. Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?

 Texnik nazorat

### 6. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating

 Zilzila, yong‘in, suv toshqini va hak.

### 9. Ro‘yxatdan o‘tish-bu…

 foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni

### 10. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

 Xavfsizlik siyosati ma’muri

### 12. Shifr nima?

 Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm

### 13. Ethernet kontsentratori qanday vazifani bajaradi?

 kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo‘naltirib beradi

### 14. Tekstni boshqa tekst ichida ma’nosini yashirib keltirish nima deb ataladi?

 steganografiya

### 15. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?

 {d, n} – yopiq, {e, n} – ochiq;

### 16. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

 1-2 jahon urushu davri

### 17. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

 Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

### 18. ……–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

 Kiberxavfsizlik

### 19. Kriptografiyaning asosiy maqsadi nima?

 maxfiylik, yaxlitlilikni ta’minlash

### 1. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.

 HandyBakcup

### 2. Makroviruslar nimalarni zararlaydi?

 Ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.

### 3. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….

 Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

### 4. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?

 Ruxsat berishga asoslangan siyosat

### 5. Nuqson atamasiga berilgan ma’noni ko‘rsating.

 Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi

### 6. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid Policy)

### 7. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuni qachon kuchga kirgan?

 1997 yil 24 aprel

### 8. Adware-zararli dastur vazifasi nimadan iborat?

 marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.

### 9. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

 Strukturalarni ruxsatsiz modifikatsiyalash

### 10. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?

 Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar

### 11. Fishing (ing. Fishing – baliq ovlash) bu…

 Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

### 12. Ma’lumotlarni zaxira nusxalash bu – …

 Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni.

### 13. ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.

 Risk monitoring

### 14. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.

 Recuva, R.saver

### 15. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

 Foydalanishni boshqarish

### 16. Kiberetika tushunchasi:

 Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

### 17. Rootkits-qanday zararli dastur?

 ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

### 18. "Fishing" tushunchasi:

 Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

### 19. Enterprise Information Security Policies, EISP-bu…

 Tashkilot axborot xavfsizligi siyosati

### 20. Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi?

 Razvedka hujumlari

### 1. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid Policy)

### 2. Spam bilan kurashishning dasturiy uslubida nimalar ko‘zda tutiladi?

 Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida filtrlanib cheklanadi.

### 3. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

 Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan

### 4. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud?

 detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar

### 5. "Axborotlashtirish to‘g‘risida"gi Qonunning maqsadi nimadan iborat?

 Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.

### 6. Ma’lumotlarni bloklarga bo‘lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?

 RAID 0

### 7. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

 Foydalanishni boshqarish

### 8. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.

 Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

### 9. Doktorlar, detektorlarga xos bo‘lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang.

 Faglar

### 10. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 1986

### 11. Rezident virus…

 tezkor xotirada saqlanadi

### 12. Zaiflik – bu…

 tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

### 13. Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi?

 Razvedka hujumlari

### 14. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

 Detektorlar

### 15. Makroviruslar nimalarni zararlaydi?

 Ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.

### 16. Texnik himoya vositаlаri – bu ...

 Texnik qurilmаlаr, komplekslаr yoki tizimlаr yordаmidа ob’ektni himoyalаshdir

### 17. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…

 Kiberjinoyat deb ataladi

### 19. Issue-Specific Security Policies, ISSP-bu…

 Muammofa qaratilgan xavfsizlik siyosati

### 20. Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.

qonunlar

### 1. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

 ABAC

### 2. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

 Xavfsizlik siyosati ma’muri

### 3. Kriptografiyaning asosiy maqsadi nima?

 maxfiylik, yaxlitlilikni ta’minlash

### 4. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?

 parol

### 5. Global simsiz tarmoqda qaysi standartlar ishlaydi?

 CDPD, 4G

### 6. Autentifikatsiya faktorlari nechta?

 3 ta

### 8. Kriptografiyada matn –bu..

 alifbo elementlarining tartiblangan to‘plami

### 9. Stenografiya ma’nosi qanday?

 sirli yozuv

### 11. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?

 Texnik vositalarning buzilishi va ishlamasligi

### 12. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

 Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

### 13. Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?

 Xesh funksiyalar

### 14. WiMAX qanday simsiz tarmoq turiga kiradi?

 Regional

### 15. Simmetrik shifrlashning noqulayligi – bu:

 Maxfiy kalitlar bilan ayirboshlash zaruriyatidir

### 16. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating

 Zilzila, yong‘in, suv toshqini va hak.

### 17. Ma’lumotlarni tasodifiy sabablar tufayli yo‘qolish sababini belgilang

 Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

### 18. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

 Biometrik autentifikatsiya

### 1. Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?

 3 taga

### 2. Kriptotizimga qo‘yiladigan umumiy talablardan biri nima?

 shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak

### 3. Autentifikatsiya faktorlari nechta?

 3 ta

### 4. Axborot xavfsizligining asosiy maqsadlaridan biri-bu…

 Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish

### 5. Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.

 Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

### 6. Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi?

 Optik tolali

### 7. Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?

 Xesh funksiyalar

### 8. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

 1-2 jahon urushu davri

### 9. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

 ABAC

### 10. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

 Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

### 11. Sub’ektga ma’lum vakolat va resurslarni berish muolajasi-bu:

 Avtorizatsiya

### 12. Kriptografiyaning asosiy maqsadi nima?

 maxfiylik, yaxlitlilikni ta’minlash

### 13. Identifikatsiya bu- …

 Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni

### 14. Fire Wall ning vazifasi...

 Tarmoqlar orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta’minlaydi

### 15. Kiberjinoyatchilik bu –. . .

 Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.

### 16. Berilgan ta’riflardan qaysi biri asimmetrik tizimlarga xos?

 Asimmetrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

### 17. Biometrik autentifikatsiyalashning avfzalliklari-bu:

 Biometrik parametrlarning noyobligi

### 18. "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?

 Foydalanish davrida maxfiylik kamayib boradi

### 19. Kriptografiyada kalitning vazifasi nima?

### 1. Spyware-qanday zararli dastur?

 Foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.

### 2. Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.

 Qonunlar

### 3. Adware-zararli dastur vazifasi nimadan iborat?

 marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.

### 4. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.

 HandyBakcup

### 5. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?

 RAID 5

### 6. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?

 Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar

### 7. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ... .

 Krakker

### 8. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?

 Paranoid siyosat

### 9. ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.

 Risk monitoring

### 10. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….

 Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

### 11. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko‘rsating?

 DDoS (Distributed Denial of Service) hujum

### 12. Kiberetika tushunchasi:

 Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

### 13. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.

 Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

### 14. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

 Foydalanishni boshqarish

### 15. Polimorf viruslar tushunchasi to‘g‘ri ko‘rsating.

 Viruslar turli ko‘rinishdagi shifrlangan viruslar bo‘lib, o‘zining ikkilik shaklini nusxadan-nusxaga o‘zgartirib boradi

### 16. Rezident virus…

 tezkor xotirada saqlanadi

### 17. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid Policy)

### 1. Kiberetika tushunchasi:

 Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

### 2. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

 Foydalanishni boshqarish

### 3. Doktorlar, detektorlarga xos bo‘lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang.

 Faglar

### 4. Zararli dasturlar qanday turlarga bo‘linadi?

 Dasturdagi zaifliklar(atayin qilingan) va zararli dasturlar(atayin qilingan)

### 5. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...

 Tamoqlararo ekranlarning o‘rnatilishi

### 6. Bag atamasini nima ma'noni beradi?

 Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo

### 7. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima deyiladi?

 Xavfsizlik siyosat

### 8. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.

 HandyBakcup

### 9. DIR viruslari nimani zararlaydi?

 FAT tarkibini zararlaydi

### 10. ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.

 Risk monitoring

### 11. Nuqson atamasiga berilgan ma’noni ko‘rsating.

 Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi

### 12. “Axborot olish kafolatlari va erkinligi to‘g‘risida”gi Qonunning 10-moddasi mazmuni qanday?

 Axborot manbaini oshkor etmaslik

### 13. Qaysi siyosat turli hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi?

 Maqbul foydalanish siyosati

### 14. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?

 Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar

### 15. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.

 Recuva, R.saver

### 16. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi?

 RAID 3

### 17. Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to‘liq tasavvurga ega shaxs kim deb ataladi?

 Xavfsizlik ma'muri (admin)

### 19. Ma’lumotlarni bloklarga bo‘lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?

 RAID 0

### 20. Qaysi siyosatda Adminstrator xavfsiz va zarur xizmatlarga indvidual ravishda ruxsat beradi?

 Extiyotkorlik siyosati

### 1. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating

 Zilzila, yong‘in, suv toshqini va hak.

### 2. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…

 login

### 3. Berilgan ta’riflardan qaysi biri asimmetrik tizimlarga xos?

 Asimmetrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

### 6. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

 1-2 jahon urushu davri

### 7. Wi-Fi necha Gs chastotali to‘lqinda ishlaydi?

 2.4-5 Gs

### 8. Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi.

 WEP, WPA, WPA2

### 11. Konfidentsiallikga to‘g‘ri ta’rif keltiring.

 axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

### 12. Autentifikatsiya nima?

 Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi

### 13. Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?

 Ma’lumotlar butunligi

### 14. ……–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

 Kiberxavfsizlik

### 15. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?

 {d, n} – yopiq, {e, n} – ochiq;

### 16. Kodlash nima?

 Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

### 17. Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq?

 simmetrik kriptotizimlar

### 18. Kriptografiyada kalitning vazifasi nima?

 Matnni shifrlash va shifrini ochish uchun kerakli axborot

### 19. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?

 Xalqa

### 20. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?

 Texnik vositalarning buzilishi va ishlamasligi

### 1. Konfidentsiallikga to‘g‘ri ta’rif keltiring.

 axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

### 2. Foydalanishni boshqarish –bu...

 Sub’ektni Ob’ektga ishlash qobilyatini aniqlashdir.

### 3. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?

 parol

### 4. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?

 Xalqa

### 5. Kodlash nima?

 Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

### 6. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?

 Yulduz

### 7. Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?

 Ma’lumotlar butunligi

### 8. Wi-Fi necha Gs chastotali to‘lqinda ishlaydi?

 2.4-5 Gs

### 9. Yaxlitlikni buzilishi bu - …

 Soxtalashtirish va o‘zgartirish

### 10. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

 1-2 jahon urushu davri

### 11. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

 Strukturalarni ruxsatsiz modifikatsiyalash

### 12. Kriptotizimga qo‘yiladigan umumiy talablardan biri nima?

 shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak

### 13. Risk nima?

 Potensial foyda yoki zarar

### 14. Assimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?

 Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun

### 15. Ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi?

 4 xil

### 16. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

 Xavfsizlik siyosati ma’muri

### 17. Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.

 Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.

### 3. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….

 Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

### 4. Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.

 Qonunlar

### 5. Rootkits-qanday zararli dastur?

 ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

### 6. Qaysi texnologiyada ma’lumotni ko‘plab nusxalari bir vaqtda bir necha disklarga yoziladi?

 RAID 1

### 7. "Axborotlashtirish to‘g‘risida"gi Qonunning maqsadi nimadan iborat?

 Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.

### 8. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid Policy)

### 10. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?

 Paranoid siyosat

### 11. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.

 "Sovuq saxiralash"

### 12. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

 Detektorlar

### 13. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ... .

 Krakker

### 14. "Fishing" tushunchasi:

 Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

### 15. O‘zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunning qaysi moddasi sabab qilib olingan?

 27(1)-modda. O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berishning alohida shartlari

### 16. Ma’lumotlarni zaxira nusxalash bu – …

 Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni.

### 17. Fishing (ing. Fishing – baliq ovlash) bu…

 Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

### 18. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 1986

### 19. "Backdoors"-qanday zararli dastur?

 zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

### 20. Kiberetika tushunchasi:

 Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

### 3. Ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi?

 4 xil

### 4. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

 Biometrik autentifikatsiya

### 5. Rol tushunchasiga ta’rif bering.

 Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin

### 6. Identifikatsiya bu- …

 Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni

### 7. Shifr nima?

 Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm

### 8. Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.

 Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

### 10. Stenografiya ma’nosi qanday?

 sirli yozuv

### 11. OSI modelida nechta sath mavjud?

 7 ta

### 12. Kriptografiyada kalitning vazifasi nima?

 Matnni shifrlash va shifrini ochish uchun kerakli axborot

### 13. Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi?

 Shaxsiy tarmoq

### 15. Risk nima?

 Potensial foyda yoki zarar

### 16. Kodlash nima?

 Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

### 17. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

 ABAC

### 18. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…

 login

### 19. Zamonaviy kriptografiya qanday bo‘limlardan iborat?

 Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish

### 1. Spam bilan kurashishning dasturiy uslubida nimalar ko‘zda tutiladi?

 Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida filtrlanib cheklanadi.

### 2. Ma’lumotlarni bloklarga bo‘lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?

 RAID 0

### 3. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.

 "Sovuq saxiralash"

### 4. Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to‘liq tasavvurga ega shaxs kim deb ataladi?

 Xavfsizlik ma'muri (admin)

### 5. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?

 RAID 5

### 6. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima deyiladi?

 Xavfsizlik siyosat

### 7. Fishing (ing. Fishing – baliq ovlash) bu…

 Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

### 8. Bag atamasini nima ma'noni beradi?

 Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo

### 9. "Backdoors"-qanday zararli dastur?

 zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

### 10. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 1986

### 11. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

 Detektorlar

### 12. Risk monitoringi ….. ni paydo bo‘lish imkoniyatini aniqlaydi.

 Yangi risklar

### 13. Ransomware qanday zarar keltiradi?

 mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi.

### 14. O‘zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunning qaysi moddasi sabab qilib olingan?

 27(1)-modda. O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berishning alohida shartlari

### 15. Texnik himoya vositаlаri – bu ...

 Texnik qurilmаlаr, komplekslаr yoki tizimlаr yordаmidа ob’ektni himoyalаshdir

### 17. Enterprise Information Security Policies, EISP-bu…

 Tashkilot axborot xavfsizligi siyosati

### 18. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?

 Paranoid siyosat

### 19. "Fishing" tushunchasi:

 Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

### 20. Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o‘z ichiga oladi?

 Xalqaro va milliy huquqiy me’yorlarni

### 1. "Fishing" tushunchasi:

 Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

### 2. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo‘naltirilgan buzg‘unchi bu - ... .

 Krakker

### 3. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?

 "Issiq zaxiralash"

### 4. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko‘rsating?

 DDoS (Distributed Denial of Service) hujum

### 5. Nuqson atamasiga berilgan ma’noni ko‘rsating.

 Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi

### 6. Risklarni identifikatsiya qilishdan maqsad nima?

 Potensial zarar yetkazadigan ehtimoliy insidentlarni prognozlash va bu zarar qay tarzda olinishi mumkinligi to‘g‘risida tasavvurga ega bo‘lish

### 7. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 1986

### 8. Rootkits-qanday zararli dastur?

 ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

### 9. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?

 Paranoid siyosat

### 10. Ko‘p platformali viruslar bu…

 Bir vaqtning o‘zida turli xildagi ob’ektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlaydi

### 11. “Axborot olish kafolatlari va erkinligi to‘g‘risida”gi Qonunning 10-moddasi mazmuni qanday?

 Axborot manbaini oshkor etmaslik

### 12. Risk monitoringi ….. ni paydo bo‘lish imkoniyatini aniqlaydi.

 Yangi risklar

### 13. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.

 Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

### 15. O‘zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunning qaysi moddasi sabab qilib olingan?

 27(1)-modda. O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berishning alohida shartlari

### 16. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?

 RAID 5

### 17. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

 Strukturalarni ruxsatsiz modifikatsiyalash

### 18. "Backdoors"-qanday zararli dastur?

 zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

### 19. Botnet-nima?

 internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi.

### 20. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

 Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan   
Windows OT lokal xavfsizlik siyosatini sozlash oynasiga o'tish uchun "Buyruqlar satri"ga quyidagi so'rovlardan qaysi biri kiritiladi?   
J:secpol.msc  
http://fayllar.org

Test savollari

1. Risk nima?

a) Potensial kuchlanish yoki zarar

b) Tasodifiy tahdid

\*c) Potensial foyda yoki zarar

d) Katta yo‘qotish

2. Tahdid nima?

a) Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa

b) Bu riskni o‘zgartiradigan harakatlar

\*c) Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa

d) Bu noaniqlikning maqsadlarga ta’siri

3. Kodlash nima?

a) Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi

b) Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi

c) Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi

\*d) Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

4. Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug‘ullanadi?

a) Kartografiya

b) Kriptoanaliz

\*c) Kriptologiya

d) Adamar usuli

5. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?

a) {d, e} – ochiq, {e, n} – yopiq;

\*b) {d, n} – yopiq, {e, n} – ochiq;

c) {e, n} – yopiq, {d, n} – ochiq;

d) {e, n} – ochiq, {d, n} – yopiq;

6. Zamonaviy kriptografiyaqanday bo‘limlardan iborat?

a) Elektron raqamli imzo; kalitlarni boshqarish;

b) Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

\*c) Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish

d) Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; kalitlarni boshqarish

7. Shifr nima?

\*a) Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm

b) Kalitlarni taqsimlash usuli

c) Kalitlarni boshqarish usuli

d) Kalitlarni generatsiya qilish usuli

8. Berilgan ta’riflardan qaysi biri Assimetrikrik tizimlarga xos?

a) Assimetrik tizimlarda k1=k2 bo‘ladi, ya’ni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi

\*b) Assimetrikrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

c) Assimetrikrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma’lum bo‘ladi, ochiq kalitni esa faqat qabul qiluvchi biladi

d) Assimetrikrik kriptotizimlarda k1≠k2 bo‘lib, kalitlar hammaga oshkor etiladi

9. Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?

a) Xabar

b) Shifrlangan xabar

c) Shifrlash

\*d) Deshifrlash

10. Axborot xavfsizligining asosiy maqsadlaridan biri-bu…

a) Ob’ektga bevosita ta’sir qilish

\*b) Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish

c) Axborotlarni shifrlash, saqlash, yetkazib berish

d) Tarmoqdagi foydalanuvchilarni xavfsizligini ta’minlab berish

11. Konfidentsiallikga to‘g‘ri ta’rif keltiring.

\*a) axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

b) axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati;

c) axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati;

d) axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati;

12. Yaxlitlikni buzilishi bu - …

\*a) Soxtalashtirish va o‘zgartirish

b) Ishonchsizlik va soxtalashtirish

c) Soxtalashtirish

d) Butunmaslik va yaxlitlanmaganlik

13. Kriptografiyaning asosiy maqsadi nima?

a) ishonchlilik, butunlilikni ta’minlash

b) autentifikatsiya, identifikatsiya

\*c) maxfiylik, yaxlitlilikni ta’minlash

d) ma’lumotlarni shaklini o‘zgartish

14. Kriptografiyada kalitning vazifasi nima?

a) Bir qancha kalitlar yig‘indisi

\*b) Matnni shifrlash va shifrini ochish uchun kerakli axborot

c) Axborotli kalitlar to‘plami

d) Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

15. Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq?

a) assimetrik kriptotizimlar

b) ochiq kalitli kriptotizimlar

\*c) simmetrik kriptotizimlar

d) autentifikatsiyalash

16. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

a) Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi

\*b) Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

c) Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin

d) Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat deshifrlash mumkin

17. Assimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?

\*a) Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun

b) ERI yaratish va tekshirish, kalitlar almashish uchun

c) Shifrlash, deshifrlash, kalitlar almashish uchun

d) Heshlash uchun

18. Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?

a) Simmetrik algoritmlar

b) Assimmetrik algoritmlar

\*c) Xesh funksiyalar

d) Kodlash

19. Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...

a) Shifrlash

b) Identifikatsiya

c) Autentifikatsiya

\*d) Avtorizatsiya

20. Autentifikatsiya faktorlari nechta?

a) 4 ta

\*b) 3 ta

c) 5 ta

d) 6 ta

21. Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

\*a) Biometrik autentifikatsiya

b) Biron nimaga egalik asosida

c) Biron nimani bilish asosida

d) Parolga asoslangan

22. Stenografiya ma’nosi qanday?

a) sirli xat

\*b) sirli yozuv

c) maxfiy axborot

d) maxfiy belgi

23. Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi?

a) Shifr matn uzunligi

\*b) Kriptobardoshlik

c) Shifrlash algoritmi

d) Texnika va texnologiyalar

24. Qog‘oz ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi?

\*a) 4 xil

b) 8 xil

c) 7 xil

d) 5 xil

25. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating

a) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

b) Zilzila, yong‘in, suv toshqini va hak.

c) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi

\*d) Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani

26. Ma’lumotlarni tasodifiy sabablar tufayli yo‘qolish sababini belgilang

\*a) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

b) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi

c) Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

d) Zilzila, yong‘in, suv toshqini va hak.

27. Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.

a) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi.

\*b) Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

c) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

d) Zilzila, yong‘in, suv toshqini va hak.

28. "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?

a) Parolni esda saqlash kerak bo‘ladi.

b) Parolni almashtirish jarayoni murakkabligi

c) Parol uzunligi soni cheklangan

\*d) Foydalanish davrida maxfiylik kamayib boradi

29. Nima uchun autentifikatsiyalashda parol ko‘p qo‘llaniladi?

a) Sarf xarajati kam, almashtirish oson

\*b) Parolni foydalanubchi ishlab chiqadi

c) Parolni o‘g‘rishlash qiyin

d) Serverda parollar saqlanmaydi

30. Elektron xujjatlarni yo‘q qilish usullari qaysilar?

a) Yoqish, ko‘mish, yanchish

\*b) Shredirlash, magnitsizlantirish, yanchish

c) Shredirlash, yoqish, ko‘mish

d) Kimyoviy usul, yoqish.

31. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.

a) Davlat tomonidan qo‘riqlanadigan va maxsus ro‘yxatlar bilan chegaralab qo‘yiladigan alohida ahamiyatli, mutlaqo maxfiy va maxfiy harbiy, siyosiy, iqtisodiy, ilmiy-texnikaviy va o‘zga xil ma’lumotlar

\*b) Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

c) Ish yuritishni tashkil etishni qo‘llaniladigan ahamiyatli, mutlaqo maxfiy ma’lumotlar

d) Muayyan jismoniy shaxsga taalluqli bo‘lgan yoki uni identifikatsiya qilish imkonini beradigan, elektron tarzda, qog‘ozda va (yoki) boshqa moddiy jismda qayd etilgan axborot

32. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?

a) Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyot.

b) Hisoblash tizimi xizmatlaridan foydalanish huqu kiberxavfsizlik qiga ega shaxs (shaxslar guruxi, tashkilot).

\*c) Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar

d) Ma’lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo‘ljallangan dasturiy va apparat vositalar

33. Axborot xavfsizligi timsollarini ko‘rsating.

a) Haker, Krakker

\*b) Alisa, Bob, Eva

c) Buzg‘unchi, hujumchi

d) sub'ekt, user

34. Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.

\*a) Qonunlar

b) Qarorlar

c) Standartlar

d) Farmonlar

35. Qaysi siyosat tizim resurslarini foydalanishda hech qanday cheklovlar qo‘ymaydi?

a) Ruxsat berishga asoslangan siyosat

b) Paranoid siyosat

c) Extiyotkorlik siyosati

\*d) Nomuntazam siyosat

36. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа xos?

a) Ruxsаt berishgа аsoslаngаn siyosаt (Permissive Policy)

b) Pаrаnoid siyosаti (Pаrаnoid Policy)

c) Ehtiyotkorlik siyosаti (Prudent Policy)

\*d) Nomuntаzаm siyosаt (Promiscuous Policy

37. Issue-Specific Security Policies, ISSP-bu…

a) Tashkilot axborot xavfsizligi siyosati

b) Tizimga qaratilgan xavfizlik siyosati

\*c) Muammofa qaratilgan xavfsizlik siyosati

d) Maqbul foydalanish siyosati

38. Qaysi siyosat turli hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi?

\*a) Maqbul foydalanish siyosati

b) Paranoid siyosat

c) Ruxsat berishga asoslangan siyosat

d) Nomuntazam siyosat

39. "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?

\*a) Foydalanish davrida maxfiylik kamayib boradi

b) Parolni esda saqlash kerak bo‘ladi

c) Parolni almashtirish jarayoni murakkabligi

d) Parol uzunligi soni cheklangan

40. (12+22)mod32– amalni bajaring.

\*a) 2

b) 12

c) 22

d) 32

41. (4\*10)mod31 – amalni bajaring.

\*a) 9

b) 12

c) 16

d) 41

42. ... - faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot.

\*a) Parol

b) Login

d) Shifrlangan axborot

43. “Dasturiy ta’minotlar xavfsizligi” bilim sohasi - bu ...

\*a) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.

b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

d) kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

44. “Jamoat xavfsizligi” bilim sohasi - bu …

\*a) u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi.

b) tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini

c) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi

d) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

45. “Ma’lumotlar xavfsizligi” bilim sohasi - bu …

\*a) ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.

b) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi

c) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

d) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

46. O‘rin almashtirish shifri bu - …

a) Murakkab bo‘lmagan kriptografik akslantirish

c) Ketma-ket ochiq matnni ustiga qo‘yish

\*d) Belgilangan biror uzunliklarga bo‘lib chiqib shifrlash

47. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

\*a) Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

b) Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi

c) Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin

d) Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin

48. O‘niga qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga mansub?

\*a) simmetrik kriptotizimlar

b) assimetrik kriptotizimlar

c) ochiq kalitli kriptotizimlar

d) autentifikatsiyalash

49. Parollash siyosatiga ko‘ra parol tanlash shartlari qanday?

a) Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo‘llanishi kerak.

b) Kamida 8 belgi; katta va kichik xavflar, sonlar qo‘llanishi kerak.

c) Kamida 6 belgi; katta xarflar, sonlar , kamida bitta maxsus simvol qo‘llanishi kerak.

d) Kamida 6 belgi; katta va kichik xarflar, kamida bitta maxsus simvol qo‘llanishi kerak.

e) Kamida 8 belgi; katta va kichik xavflar, sonlar qo‘llanishi kerak.

50. RSA algoritmi qanday jarayonlardan tashkil topgan?

\*a) Kalitni generatsiyalash; Shifrlash; Deshifrlash.

b) Shifrlash; Imzoni tekshirish; Deshifrlash

c) Kalitni generatsiyalash; imzolash; Deshifrlash.

d) Imzoni tekshirish ; Shifrlash; Deshifrlash.

51. RSA qanday algoritm?

a) Raqamli imzo algoritmi

b) Shifrlash algoritmi

c) Kalitli almashish algoritmi

d) Shifrlash algoritmi va kalitli almashish algoritmi

52. Shaxsning, o‘zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, axborot-kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu?

a) login

b) parol

c) identifikatsiya

d) maxfiy maydon

53. Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi?

\*a) Kriptobardoshlik

b) Shifr matn uzunligi

d) Texnika va texnologiyalar

54. Shifrlash qanday jarayon?

\*a) akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi

b) kalit asosida shifrmatn ochiq matnga akslantiriladi

c) shifrlashga teskari jarayon

d) almashtirish jarayoni bo‘lib: ochiq matn deb nomlanadigan matn o‘girilgan holatga almashtiriladi

55. Smart karta o‘lchamidagi, kichik xajmdagi xotira va xisoblash imkoniyatiga ega bo‘lgan, o‘zida parol yoki kalitni saqlovchi qurilma nima deb ataladi?

a) Token, Smartkarta

b) Chip

c) Fleshka

d) Disk

56. Cisco tashkiloti esa kiberxavfsizlikka qanday ta’rif bergan?

\*a) Kiberxavfsizlik - tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti

b) hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan

c) Bu yozilgan va xabar qilingan ma’luotlarning haqiqiyligini, to‘g‘riligini, butunligini saqlash qobiliyati

d) Ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.

57. Foydalanuvchanlik-bu…

\*a) avtorizatsiyalangan mantiqiy obyekt so‘rovi bo‘yicha axborotning tayyorlik va foydalanuvchanlik holatida bo‘lishi xususiyati

b) axborotning buzilmagan ko‘rinishida (axborotning qandaydir qayd etilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati

c) axborot yoki uni eltuvchisining shunday holatiki, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi

d) potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi

58. Kiberxavfsizlik bilim sohasi nechta bilim sohasini o‘z ichiga oladi?

\*a) 8 ta

b) 7 ta

c) 6 ta

d) 5 ta

59. Axborotdan oqilona foydalanish kodeksi nechanchi yil ishlab chiqilgan?

a) 1973 yil

b) 1980 yil

c) 1991 yil

\*d) 2002 yil

60. Ijtimoiy (sotsial) injineriya-bu…

a) turli psixologik usullar va firibgarlik amaliyotining to‘plami, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olish

b) Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish

c) axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi

d) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

61. Kiberxavfsizlik arxitekturasi nechta sathga ajratiladi?

\*a) 3ta

b) 2 ta

c) 4 ta

d) 5 ta

62. Tashkilot axborot xavfsizligi siyosati-bu…

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. Bundan tashqari, ushbu siyosat taklif etilgan va talab qilingan axborot xavfsizligi strukturasi talablarini kafolatlaydi

b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. Unda profílaktik choralar, masalan, foydalanuvchilarning foydalanish huquqini avtorizasiyalash uchun zarur bo‘lgan texnologiyalar ko‘rsatiladi

63. Muammoga qaratilgan xavfsizlik siyosatlari …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. Bundan tashqari, ushbu siyosat taklif etilgan va talab qilingan axborot xavfsizligi strukturasi talablarini kafolatlaydi

b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. Unda profílaktik choralar, masalan, foydalanuvchilarning foydalanish huquqini avtorizasiyalash uchun zarur bo‘lgan texnologiyalar ko‘rsatiladi

c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi. Bunda tashkilotlar tizimni madadlash maqsadida muolajalar va standartlarni o‘z ichiga oigan SSSP siyosatini ishlab chiqadilar va boshqaradilar. Bundan tashqari, tashkilot tomonidan foydalanilgan texnologiyalar tizimga qaratilgan siyosatlarni o‘z ichiga oladi

d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi. Internetdan foydalanish siyosati o‘z ichiga Internetdan foydalanish ruxsati, tizim xavfsizligi, tarmoqni o‘rnatish, AT xizmati va boshqa yo‘riqnomalarni qamrab oladi

64. Tizimga qaratilgan xavfsizlik siyosatlari …

b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. Unda profílaktik choralar, masalan, foydalanuvchilarning foydalanish huquqini avtorizasiyalash uchun zarur bo‘lgan texnologiyalar ko‘rsatiladi

c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi. Bunda tashkilotlar tizimni madadlash maqsadida muolajalar va standartlarni o‘z ichiga oigan SSSP siyosatini ishlab chiqadilar va boshqaradilar. Bundan tashqari, tashkilot tomonidan foydalanilgan texnologiyalar tizimga qaratilgan siyosatlarni o‘z ichiga oladi

d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi. Internetdan foydalanish siyosati o‘z ichiga Internetdan foydalanish ruxsati, tizim xavfsizligi, tarmoqni o‘rnatish, AT xizmati va boshqa yo‘riqnomalarni qamrab oladi

65. Internetdan foydalanish siyosati. …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. Bundan tashqari, ushbu siyosat taklif etilgan va talab qilingan axborot xavfsizligi strukturasi talablarini kafolatlaydi

b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. Unda profílaktik choralar, masalan, foydalanuvchilarning foydalanish huquqini avtorizasiyalash uchun zarur bo‘lgan texnologiyalar ko‘rsatiladi

c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi. Bunda tashkilotlar tizimni madadlash maqsadida muolajalar va standartlarni o‘z ichiga oigan SSSP siyosatini ishlab chiqadilar va boshqaradilar. Bundan tashqari, tashkilot tomonidan foydalanilgan texnologiyalar tizimga qaratilgan siyosatlarni o‘z ichiga oladi

\*d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi. Internetdan foydalanish siyosati o‘z ichiga Internetdan foydalanish ruxsati, tizim xavfsizligi, tarmoqni o‘rnatish, AT xizmati va boshqa yo‘riqnomalarni qamrab oladi

66. Ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o‘zgartirishlar oilasi-…

\*a) Kriptotizim

b) Deshifrlash

c) Rasshifrovkalash

d) Shifrlash

67. O‘zgartirishlar oilasidan birini tanlashni ta’minlovchi kriptografik algoritmning qandaydir parametrlarining muayyan qiymati-…

a) Kriptotizim

b) Kalit

\*c) Rasshifrovkalash

d) Shifrlash

68. Kiberjinoyat qanday turlarga bo‘linadi?

\*a) ichki va tashqi

b) Faol va passiv

c) Asosiy va quyi

d) Xalqaro va milliy

69. Autentifikatsiya nima?

a) Tizim me’yoriy va g‘ayritabiiy hollarda rejalashtirilgandek o‘zini tutishligi holati

b) Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi

c) Istalgan vaqtda dastur majmuasining mumkinligini kafolati

d) Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi

70. Identifikatsiya bu- …

\*a) Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni

b) Ishonchliligini tarqalishi mumkin emasligi kafolati

c) Axborot boshlang‘ich ko‘rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o‘zgarishlar

d) Axborotni butunligini saqlab qolgan holda uni elementlarini o‘zgartirishga yo‘l qo‘ymaslik

71. Kriptologiya –qanday fan?

a) axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

b) kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi

c) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

\*d) axborotni qayta akslantirib himoyalash muammosi bilan shug‘ullanadi

72. Kriptobardoshlilik deb nimaga aytilladi?

\*a) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

b) axborotni qayta akslantirib himoyalash muammosi bilan shug‘ullanadi

c) kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi

d) axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

73. Kriptografiyada matn –bu..

a) matnni shifrlash va shifrini ochish uchun kerakli axborot

\*c) alifbo elementlarining tartiblangan to‘plami

d) kalit axborotni shifrlovchi kalitlar

74. Kriptotizimga qo‘yiladigan umumiy talablardan biri nima?

a) shifrlash algoritmining tarkibiy elementlarini o‘zgartirish imkoniyati bo‘lishi lozim

b) ketma-ket qo‘llaniladigan kalitlar o‘rtasida oddiy va oson bog‘liqlik bo‘lishi kerak

c) shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak

d) maxfiylik o‘ta yuqori darajada bo‘lmoqligi lozim

75. “Kiberxavfsizlik to‘g‘risida” Qonun qachon tasdiqlangan?

a) 15.04.2022

b) 20.03.2021

c) 02.01.2000

d) 15.01.1995

76. Kiberjinoyatchilik bu –. . .

\*a) Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.

b) Kompyuter o‘yinlari

c) Faqat banklardan pul o‘g‘irlanishi

d) Autentifikatsiya jarayonini buzish

77. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

a) Tabiy ofat va avariya

\*c) Strukturalarni ruxsatsiz modifikatsiyalash

d) Foydalanuvchilar va xizmat ko‘rsatuvchi hodimlarning hatoliklari

78. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?

a) Axborotdan ruhsatsiz foydalanish

b) Zararkunanda dasturlar

c) An’anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili

d) Texnik vositalarning buzilishi va ishlamasligi

79. Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?

a) Axborotning konfedentsialligi

b) Foydalanuvchanligi

\*c) Ma’lumotlar butunligi

d) Ixchamligi

80. Biometrik autentifikatsiyalashning avfzalliklari-bu:

a) Bir marta ishlatilishi

b) Biometrik parametrlarning noyobligi

c) Biometrik parametrlarni o‘zgartirish imkoniyati

d) Autentifikatsiyalash jarayonining soddaligi

81. Simmetrik shifrlashning noqulayligi – bu:

a) Maxfiy kalitlar bilan ayirboshlash zaruriyatidir

b) Kalitlar maxfiyligi

c) Kalitlar uzunligi

d) Shifrlashga ko‘p vaqt sarflanishi va ko‘p yuklanishi

82. Token, smartkartalarda xavfsizlik tomonidan kamchiligi nimada?

a) Foydalanish davrida maxfiylik kamayib boradi

b) Qurilmalarni ishlab chiqarish murakkab jarayon

c) Qurilmani yo‘qotilishi katta xavf olib kelishi mumkin

83. Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?

a) 4 taga

b) 2 taga

c) 5 taga

\*d) 3 taga

84. Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi?

\*a) Onx458&hdsh)

b) 12456578

c) salomDunyo

d) Mashina777

85. Parollash siyosatiga ko‘ra parol tanlash shartlari qanday?

a) Kamida 8 belgi; katta va kichik xavflar, sonlar qo‘llanishi kerak.

\*b) Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo‘llanishi kerak.

c) Kamida 6 belgi; katta xarflar, sonlar , kamida bitta maxsus simvol qo‘llanishi kerak.

d) Kamida 6 belgi; katta va kichik xarflar, kamida bitta maxsus simvol qo‘llanishi kerak.

86. MD5, SHA1, SHA256, O‘z DSt 1106:2009- qanday algoritmlar deb ataladi?

a) Kodlash

b) Xeshlash

c) Shifrlash

d) Stenografiya

87. RSA algoritm qaysi yilda ishlab chiqilgan?

a) 1977 yil

b) 1966 yil

c) 1988 yil

d) 1956 yil

88. Windows OT lokal xavfsizlik siyosatini sozlash oynasiga o‘tish uchun buyruqlar satrida qaysi buyruq yoziladi?

a) secpol.msc

b) regedit

c) chkdsk

d) diskcopy

89. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

a) O‘rta asr davrida

b) 15 asr davrida

\*c) 1-2 jahon urushu davri

d) 21 asr davrida

90. "Fishing" tushunchasi:

a) Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

b) Kompyuter, dasturlar va tarmoqlar xavfsizligi

\*c) Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

d) Kompyuter tizimlariga ruxsatsiz ta’sir ko‘rsatish

91. BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?

Javob… AES, Serpent, Twofish

92. Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda

qo‘llaniladi?

93. Qaysi siyosatga ko‘ra hamma narsa taqiqlanadi?

Javob… \*Paranoid siyosat

94. Assimetrikrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun nechta

kalit ishlatiladi?

Javob. Ikkita kalit  
 95. Masofadan ERI olish uchun qaysi internet manzilga murojaat qilinadi?

Javob. mygov.uz

96. Maxfiy xabarni sohta xabar ichiga berkitish orqali aloqani yashirish nima deb ataladi?

Javob. Steganografiya

97. Tizim xavfsizligi” bilim sohasi - bu …

javob : tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi.

98. Axborot qanday sifatlarga ega bo‘lishi kerak?

J: ishonchli, qimmatli va to’liq

99. Smart karta o‘lchamidagi, kichik xajmdagi xotira va xisoblash imkoniyatiga ega bo‘lgan,

o‘zida parol yoki kalitni saqlovchi qurilma nima deb ataladi?

J: Token, Smartkarta

100. ......–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan

sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni

mujassamlashtirgan.

J: Kiberxavfsizlik

101. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan

belgilar ketma-ketligi (maxfiy so‘z) – nima?

J: Parol

102. Muammoga qaratilgan xavfsizlik siyosatlari …

J: bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik

siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga

bog‘liq bo‘ladi. Unda profílaktik choralar, masalan, foydalanuvchilarning foydalanish huquqini

avtorizasiyalash uchun zarur bo‘lgan texnologiyalar ko‘rsatiladi

103. Elektron raqamli imzo kalitlari ro‘yxatga olish qaysi tashkilot tomonidan bajariladi

J: Sertifikatlari roʻyxatga olish markazlari

104. Kriptologiyani fan sifatida shakllanishida nechta davrlarga bo‘linadi?

J: 4 ga

105. Kriptografiyada "alifbo" deganda nima tushuniladi?

J:axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam

106.Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?

J:Imzo qo‘yish va imzoni tekshirishdan

107.Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar

bloklanadi?

J: Ruxsat berishga asoslangan siyosat

108. Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi?

J: tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi

109. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…

J: login

Konfidentsiallikga to‘g‘ri ta’rif keltiring.====

#axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; ====

axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati; ====

axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanmaganligi; ====

axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati;

++++

Yaxlitlikni buzilishi bu - …====

#Soxtalashtirish va o‘zgartirish====

Ishonchsizlik va soxtalashtirish====

Soxtalashtirish====

Butunmaslik va yaxlitlanmaganlik

++++

Kriptografiyaning asosiy maqsadi nima? ====

ishonchlilik, butunlilikni ta’minlash====

autentifikatsiya, identifikatsiya====

#maxfiylik, yaxlitlilikni ta’minlash====

ma’lumotlarni shaklini o‘zgartish

++++

Kriptografiyada kalitning vazifasi nima? ====

Bir qancha kalitlar yig‘indisi====

#Matnni shifrlash va shifrini ochish uchun kerakli axborot====

Axborotli kalitlar to‘plami====

Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

++++

Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq? ====

assimetrik kriptotizimlar====

ochiq kalitli kriptotizimlar====

#simmetrik kriptotizimlar====

autentifikatsiyalash

++++

Autentifikatsiya nima? ====

Tizim me’yoriy va g‘ayritabiiy hollarda rejalashtirilgandek o‘zini tutishligi holati====

#Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi====

Istalgan vaqtda dastur majmuasining mumkinligini kafolati====

Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi

++++

Identifikatsiya bu- …====

#Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni====

Ishonchliligini tarqalishi mumkin emasligi kafolati====

Axborot boshlang‘ich ko‘rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o‘zgarishlar====

Axborotni butunligini saqlab qolgan holda uni elementlarini o‘zgartirishga yo‘l qo‘ymaslik

++++

Kriptologiya –qanday fan? ====

axborotni qayta akslantirishning fizik usullarini ishlab chiqadi ====

kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi====

kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi====

#axborotni qayta akslantirib himoyalash muammosi bilan shug‘ullanadi

++++

Kriptobardoshlilik deb nimaga aytilladi? ====

#kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi====

axborotni qayta akslantirib himoyalash muammosi bilan shug‘ullanadi====

kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi====

axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

++++

Kriptografiyada matn –bu.. ====

matnni shifrlash va shifrini ochish uchun kerakli axborot====

axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam====

#alifbo elementlarining tartiblangan to‘plami====

kalit axborotni shifrlovchi kalitlar

++++

Kriptotizimga qo‘yiladigan umumiy talablardan biri nima? ====

shifrlash algoritmining tarkibiy elementlarini o‘zgartirish imkoniyati bo‘lishi lozim====

ketma-ket qo‘llaniladigan kalitlar o‘rtasida oddiy va oson bog‘liqlik bo‘lishi kerak====

#shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak====

maxfiylik o‘ta yuqori darajada bo‘lmoqligi lozim

++++

Berilgan ta’riflardan qaysi biri Assimetrikrik tizimlarga xos? ====

Assimetrikrik tizimlarda k1=k2 bo‘ladi, ya’ni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi====

#Assimetrikrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi====

Assimetrikrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma’lum bo‘ladi, ochiq kalitni esa faqat qabul qiluvchi biladi====

Assimetrikrik kriptotizimlarda k1≠k2 bo‘lib, kalitlar hammaga oshkor etiladi

++++

Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…====

parol====

#login====

identifikatsiya====

token

++++

Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima? ====

login====

#parol====

identifikatsiya====

maxfiy maydon

++++

Ro‘yxatdan o‘tish-bu…====

#foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni====

axborot tizimlari ob’yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo‘yicha solishtirib uni aniqlash jarayoni====

ob’ekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash====

foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

++++

Axborot qanday sifatlarga ega bo‘lishi kerak? ====

uzluksiz va uzlukli====

ishonchli, qimmatli va uzlukli====

#ishonchli, qimmatli va to‘liq====

ishonchli, qimmatli va uzluksiz

++++

Maxfiy xabarni sohta xabar ichiga berkitish orqali aloqani yashirish nima deb ataladi?====

sirli yozuv====

#steganografiya====

skrembler====

shifr mashinalar

++++

Kriptologiyani fan sifatida shakllanishida nechta davrlarga bo‘linadi?====

#4 ga====

3 ga====

2 ga====

5 ga

++++

Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? ====

Xabar====

Shifrlangan xabar====

Shifrlash====

#Deshifrlash

++++

Risk nima? ====

Potensial kuchlanish yoki tahdid====

Tasodifiy tahdid====

#Potensial foyda yoki zarar====

Katta yo‘qotish

++++

Tahdid nima? ====

Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa====

Bu riskni o‘zgartiradigan harakatlar====

#Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa====

Bu noaniqlikning maqsadlarga ta’siri

++++

Kodlash nima? ====

Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi

mumkin bo‘ladi====

Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi

mumkin bo‘ladi====

Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi====

#Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

++++

Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug‘ullanadi? ====

Kartografiya====

#Kriptoanaliz====

Kriptologiya====

Adamar usuli

++++

Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi? ====

{d, e} – ochiq, {e, n} – yopiq; ====

#{d, n} – yopiq, {e, n} – ochiq; ====

{e, n} – yopiq, {d, n} – ochiq; ====

{e, n} – ochiq, {d, n} – yopiq;

++++

Zamonaviy kriptografiya qanday bo‘limlardan iborat? ====

Elektron raqamli imzo; kalitlarni boshqarish;====

Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; ====

#Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish ====

Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; kalitlarni boshqarish

++++

Shifr nima?====

#Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm ====

Kalitlarni taqsimlash usuli====

Kalitlarni boshqarish usuli ====

Kalitlarni generatsiya qilish usuli

++++

Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? ====

Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi====

#Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi====

Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin====

Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat deshifrlash mumkin

++++

Assimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? ====

#Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun====

ERI yaratish va tekshirish, kalitlar almashish uchun====

Shifrlash, deshifrlash, kalitlar almashish uchun====

Heshlash uchun

++++

Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi? ====

Simmetrik algoritmlar====

Assimmetrik algoritmlar====

#Xesh funksiyalar====

Kodlash

++++

Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu... ====

Shifrlash====

Identifikatsiya====

Autentifikatsiya====

#Avtorizatsiya

++++

Autentifikatsiya faktorlari nechta? ====

4 ta====

#3 ta====

5 ta====

6 ta

++++

Ko‘z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar? ====

#Biometrik autentifikatsiya====

Biron nimaga egalik asosida====

Biron nimani bilish asosida====

Parolga asoslangan

++++

Stenografiya ma’nosi qanday? ====

sirli xat====

#sirli yozuv====

maxfiy axborot====

maxfiy belgi

++++

Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi? ====

Shifr matn uzunligi====

#Kriptobardoshlik====

Shifrlash algoritmi====

Texnika va texnologiyalar

++++

Qog‘oz ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi? ====

#4 xil====

8 xil====

7 xil====

5 xil

++++

Kiberjinoyat qanday turlarga bo‘linadi?====

#ichki va tashqi====

Faol va passiv====

Asosiy va quyi====

Xalqaro va milliy

++++

“Kiberxavfsizlik to‘g‘risida” Qonun qachon tasdiqlangan?====

#15.04.2022====

20.03.2021====

02.01.2000====

15.01.1995

++++

Kiberjinoyatchilik bu –. . . ====

#Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. ====

Kompyuter o‘yinlari====

Faqat banklardan pul o‘g‘irlanishi====

Autentifikatsiya jarayonini buzish

++++

Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi? ====

Tabiy ofat va avariya====

Texnik vositalarning buzilishi va ishlamasligi====

#Strukturalarni ruxsatsiz modifikatsiyalash====

Foydalanuvchilar va xizmat ko‘rsatuvchi hodimlarning hatoliklari

++++

Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi? ====

Axborotdan ruhsatsiz foydalanish====

Zararkunanda dasturlar====

An’anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili====

#Texnik vositalarning buzilishi va ishlamasligi

++++

Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi? ====

Axborotning konfedentsialligi====

Foydalanuvchanligi====

#Ma’lumotlar butunligi====

Ixchamligi

++++

Simmetrik shifrlashning noqulayligi – bu:====

#Maxfiy kalitlar bilan ayirboshlash zaruriyatidir====

Kalitlar maxfiyligi====

Kalitlar uzunligi====

Shifrlashga ko‘p vaqt sarflanishi va ko'p yuklanishi

++++

Token, smartkartalarda xavfsizlik tomonidan kamchiligi nimada? ====

Foydalanish davrida maxfiylik kamayib boradi====

Qurilmalarni ishlab chiqarish murakkab jarayon====

#Qurilmani yo'qotilishi katta xavf olib kelishi mumkin====

Qurilmani qalbakilashtirish oson

++++

Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating====

Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi====

#Zilzila, yong‘in, suv toshqini va hak====

Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi====

Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani

++++

Ma’lumotlarni tasodifiy sabablar tufayli yo‘qolish sababini belgilang====

#Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi====

Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi====

Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. ====

Zilzila, yong‘in, suv toshqini va hak.

++++

Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang. ====

Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi. ====

#Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. ====

Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi====

Zilzila, yong‘in, suv toshqini va hak

++++

Nima uchun autentifikatsiyalashda parol ko‘p qo‘llaniladi? ====

#Sarf xarajati kam, almashtirish oson====

Parolni foydalanubchi ishlab chiqadi====

Parolni o‘g‘rishlash qiyin====

Serverda parollar saqlanmaydi

++++

Elektron xujjatlarni yo‘q qilish usullari qaysilar? ====

Yoqish, ko‘mish, yanchish====

#Shredirlash, magnitsizlantirish, yanchish====

Shredirlash, yoqish, ko‘mish====

Kimyoviy usul, yoqish.

++++

Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan? ====

4 taga====

2 taga====

5 taga====

#3 taga

++++

Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi? ====

#Onx458&hdsh) ====

12456578====

salomDunyo====

Mashina777

++++

Parollash siyosatiga ko'ra parol tanlash shartlari qanday? ====

Kamida 8 belgi; katta va kichik xavflar, sonlar qo'llanishi kerak. ====

#Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. ====

Kamida 6 belgi; katta xarflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. ====

Kamida 6 belgi; katta va kichik xarflar, kamida bitta maxsus simvol qo'llanishi kerak.

++++

MD5, SHA1, SHA256, O‘z DSt 1106:2009- qanday algoritmlar deb ataladi? ====

Kodlash====

#Xeshlash====

Shifrlash====

Stenografiya

++++

RSA algoritm qaysi yilda ishlab chiqilgan? ====

#1977 yil====

1966 yil====

1988 yil====

1956 yil

++++

Windows OT lokal xavfsizlik siyosatini sozlash oynasiga o'tish uchun buyruqlar satrida qaysi buyruq yoziladi? ====

#secpol.msc====

regedit====

chkdsk====

diskcopy

++++

Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi? ====

O‘rta asr davrida====

15 asr davrida====

#1-2 jahon urushu davri====

21 asr davrida

++++

"Fishing" tushunchasi:====

Kompyuter va kompyuter tarmoqlarida odamlarning etikasi====

Kompyuter, dasturlar va tarmoqlar xavfsizligi====

#Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi====

Kompyuter tizimlariga ruxsatsiz ta’sir ko'rsatish

+++++

“Elektron hujjat” tushunchasi haqida to‘g’ri ta’rif berilgan qatorni ko‘rsating.====

Davlat tomonidan qo'riqlanadigan va maxsus ro'yxatlar bilan chegaralab qo'yiladigan alohida ahamiyatli, mutlaqo maxfiy va maxfiy harbiy, siyosiy, iqtisodiy, ilmiy-texnikaviy va o'zga xil ma’lumotlar====

#Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo'lgan axborot elektron hujjatdir====

Ish yuritishni tashkil etishni qo‘llaniladigan ahamiyatli, mutlaqo maxfiy ma’lumotlar====

Muayyan jismoniy shaxsga taalluqli bo'lgan yoki uni identifikatsiya qilish imkonini beradigan, elektron tarzda, qog'ozda va (yoki) boshqa moddiy jismda qayd etilgan axborot

+++++

Axborot xavfsizligi boshqaruv tizimida "Aktiv" so'zi nimani anglatadi?====

Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyot.====

Hisoblash tizimi xizmatlaridan foydalanish huqu kiberxavfsizlik qiga ega shaxs (shaxslar guruxi, tashkilot).====

#Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar====

Ma’lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo'ljallangan dasturiy va apparat vositalar

+++++

Axborot xavfsizligi timsollarini ko'rsating.====

Haker, Krakker, user====

#Alisa, Bob, Eva====

Buzg'unchi, hujumchi====

sub'ekt, user

+++++

Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.====

#Qonunlar====

Qarorlar====

Standartlar====

Farmonlar

++++

Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа xos?====

Ruxsаt berishgа аsoslаngаn siyosаt (Permissive Policy)====

#Pаrаnoid siyosаti (Pаrаnoid Policy)====

Ehtiyotkorlik siyosаti (Prudent Policy)====

Nomuntаzаm siyosаt (Promiscuous Policy

+++++

Kompyuter yoki boshqa qurilmalarga qarshi qilingan va boshqa qurilmalar orqali qilingan jinoyat-…====

Kibersport deb ataladi====

Kiberterror deb ataladi====

#Kiberjinoyat deb ataladi====

Kiberataka deb ataladi

+++++

Qaysi siyosat turli hisoblash resurslaridan to'g'ri foydalanishni belgilaydi?====

#Maqbul foydalanish siyosati====

Paranoid siyosat====

Ruxsat berishga asoslangan siyosat====

Nomuntazam siyosat

+++++

Qaysi siyosatda Adminstrator xavfsiz va zarur xizmatlarga indvidual ravishda ruxsat beradi?====

Paranoid siyosat====

Ruxsat berishga asoslangan siyosat====

Nomuntazam siyosat====

#Extiyotkorlik siyosati

+++++

Qaysi siyosatga ko'ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?====

Nomuntazam siyosat====

Paranoid siyosat====

#Ruxsat berishga asoslangan siyosat====

Extiyotkorlik siyosati

+++++

Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to'plami nima deyiladi?====

#Xavfsizlik siyosat====

Standart====

Qonun====

Buyruq

+++++

Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to'liq tasavvurga ega shaxs kim deb ataladi?====

Xavfsizlik mutaxasisi====

Rahbar====

Foydalanuvchi====

#Xavfsizlik ma'muri (admin)

+++++

Ehtiyotkorlik siyosati (Prudent Policy) – bu ….====

Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi====

Hamma narsa ta’qiqlanadi====

Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi====

#Barcha hizmatlar blokirovka qilingandan so‘ng bog’lanadi

+++++

(12+22)mod32– amalni bajaring. ====

#2====

12====

22====

32

++++

(4\*10)mod31 – amalni bajaring. ====

#9====

12====

16====

41

++++

... - faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot====

#Parol ====

Login====

Maxfiy kalit ====

Shifrlangan axborot

++++

“Dasturiy ta’minotlar xavfsizligi” bilim sohasi - bu ... ====

#foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi. ====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi. ====

tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi. ====

kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

++++

“Jamoat xavfsizligi” bilim sohasi - bu … ====

#u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi. ====

tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini====

foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

++++

“Ma’lumotlar xavfsizligi” bilim sohasi - bu …====

#ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.====

foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.====

tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

++++

“Tizim xavfsizligi” bilim sohasi - bu …====

#tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi.====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.====

tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.====

kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.

++++

“Xodim xavfsizligi” tushunchasi- bu…====

#Qandaydir jiddiy axborotdan foydalanish imkoniyatiga ega barcha xodimlarning kerakli avtorizatsiyaga va barcha kerakli ruxsatnomalarga egalik kafolatini ta’minlovchi usul.====

Axborot tarmog'ini ruxsatsiz foydalanishdan, me’yoriy harakatiga tasodifan aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.====

Destruktiv harakatlarga va yolg'on axborotni zo'rlab qabul qilinishiga olib keluvchi ishlanadigan va saqlanuvchi axborotdan ruxsatsiz foydalanishga urinishlarga kompyuter tizimining qarshi tura olish hususiyati.====

Korxona o'z faoliyatini buzilishsiz va to'xtalishsiz yurgiza oladigan vaqt bo'yicha barqaror bashoratlanuvchi atrof-muhit holati.

++++

“Yaxlitlik” atamasiga berilgan ta’rifni belgilang.====

#Bu yozilgan va xabar qilingan ma’luotlarning haqiqiyligini, to‘g’riligini, butunligini saqlash qobiliyati====

Funksionala imkoniyatni o‘z vaqtida foydalanish====

Tizimning ruxsat berilgan foydalanish uchun ma’lumot tarqatishni cheklash====

Korxona o'z faoliyatini buzilishsiz va to'xtalishsiz yurgiza oladigan vaqt bo'yicha barqaror bashoratlanuvchi atrof-muhit holati

++++

……–hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.====

#Kiberxavfsizlik====

Axborot xavfsizligi====

Kiberjtnoyatchilik====

Risklar

++++

Assimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? ====

#shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun====

shifrlash, deshifrlash====

ERI yaratish va tekshirish, kalitlar almashish uchun====

shifrlash, deshifrlash, kalitlar almashish uchun

++++

Assimetrikrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun nechta kalit ishlatiladi? ====

#Ikkita kalit====

Bitta kalit====

Elektron raqamli imzo====

Foydalanuvchi identifikatori

++++

Autentifikatsiya jarayoni qanday jarayon? ====

#obyekt yoki subyektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy axborotni tekshirish orqali asilligini aniqlash====

axborot tizimlari obyekt va subyektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo‘yicha solishtirib uni aniqlash jarayoni====

foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni====

foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni

++++

Avtorizatsiya nima? ====

#Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilarga tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni====

Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni====

Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni====

Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilar

++++

Axborot o‘lchovini kamayish tartibini to‘g’ri tanlang====

#Gigabayt,megabayt,kilobayt====

Bit,bayt,kilobayt,megabayt====

Gigabayt,megabayt,pikobayt====

Gigabayt,pikobayat,terobayt

++++

Axborot o‘lchovini o‘sish tartibini to‘g’ri tanlang====

#Bayt,kilobayt,megabayt====

Bit,bayt,megabayt,kilobayt====

Gigabayt,megabayt,pikobayt====

Gigabayt,megabayt,pikobayt

++++

Axborot xavfsizligi boshqaruv tizimida "Aktiv" so'zi nimani anglatadi? ====

#Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar====

Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyot. ====

Hisoblash tizimi xizmatlaridan foydalanish huquqiga ega shaxs (shaxslar guruxi, tashkilot). ====

Ma’lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo'ljallangan dasturiy va apparat vositalar

++++

Axborot xavfsizligi qanday asosiy xarakteristikalarga ega? ====

#Butunlik, konfidentsiallik, foydalana olishlik====

Butunlik, himoya, ishonchlilikni urganib chiqishlilik====

Konfidentsiallik, foydalana olishlik====

Himoyalanganlik, ishonchlilik, butunlik

++++

Axborot xavfsizligining huquqiy ta'minotiga nimalar kiradi? ====

#Qonunlar, aktlar, me'yoriy-huquqiy hujjatlar, qoidalar, yo'riqnomalar, qo'llanmalar majmui====

Qoidalar yo'riqnomalar, tizim arxetikturasi, xodimlar malakasi, yangi qoidalar, yangi yo'riqnomalar, qo'llanmalar majmui====

Qoidalar, yo'riqnomalar, tizim strukturasi, dasturiy ta’minot====

Himoya tizimini loyihalash, nazorat usullari

++++

Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi? ====

#Ma’lumotlar butunligi====

Axborotning konfedentsialligi====

Foydalanuvchanligi====

Ixchamligi

++++

"Barcha xizmatlar blokirovka qilingandan so‘ng bog’lanadi". -Bu qaysi xavfsizlik siyosatiga hos? ====

#Ehtiyotkorlik siyosati (Prudent Policy)====

Nomuntazam siyosat (Promiscuous Policy) ====

Paranoid siyosati (Paranoid Policy) ====

Ruxsat berishga asoslangan siyosat (Permissive Policy)

++++

BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? ====

#AES, Serpent, Twofish====

Pleyfer, Sezar====

DES, sezar, Futurama ====

AES, Serpent, Twofish, Triple DES, GOST 28147-89

++++

Elektron pochtaga kirishda foydalanuvchi qanday autetntifikasiyalashdan o‘tadi? ====

#Parol asosida====

Smart karta asosida====

Biometrik asosida====

Ikki tomonlama

++++

Elektron raqamli imzo - bu …====

#xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimcha====

matnni shifrlash va shifrini ochish uchun kerakli axborot====

axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam====

kalit axborotni shifrlovchi kalitlar

++++

Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? ====

#Imzo qo‘yish va imzoni tekshirishdan====

Faqat imzo qo‘yishdan====

Faqat imzoni tekshirishdan====

Kalitlarni taqsimlashdan

++++

Elektron raqamli imzo kalitlari ro'yxatga olish qaysi tashkilot tomonidan bajariladi====

#Sertifikatlari roʻyxatga olish markazlari====

Tegishli Vazirliklar====

Axborot xavfsizligi markazlari====

Davlat Hokimiyati

++++

Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima? ====

#Autentifikatsiya ====

Identifikatsiya ====

Avtorizatsiya ====

Ma’murlash

++++

Kalit – bu …====

#Matnni shifrlash va shifrini ochish uchun kerakli axborot====

Bir qancha kalitlar yig’indisi====

Axborotli kalitlar to‘plami====

Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

++++

Kiberetika tushunchasi====

#Kompyuter va kompyuter tarmoqlarida odamlarning etikasi====

Kompyuter, dasturlar va tarmoqlar xavfsizligi====

Kompyuter tizimlariga ruxsatsiz ta’sir ko'rsatish====

Tashkilot va odamlarning mahsus va shahsiy ma’lumotlarini olishka qaratilgan internet-atakasi

++++

Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi? ====

#tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi ====

tashkilot xodimlari himoyasini ta’minlaydi ====

tashkilot axborotlari va binolarining himoyasini ta’minlaydi ====

tashkilot omborini va axborotlari himoyasini ta’minlaydi

++++

Ko‘z pardasi, yuz tuzilishi, ovoz tembri - bu tushunchalar qaysi autentifikatsiya turiga mansub? ====

#Biometrik autentifikatsiya ====

Biron nimani bilish asosida====

Biron nimaga egalik asosida====

Gibrid

++++

Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda qo'llaniladi? ====

#ochiq kalitlar====

yopiq kalitlar====

seans kalitlari====

Barcha tutdagi kalitlar

++++

Kriptografiyada "alifbo" deganda nima tushuniladi? ====

#axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam====

matnni shifrlash va shifrini ochish uchun kerakli axborot====

xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimcha====

kalit axborotni shifrlovchi kalitlar

++++

Kriptografiyada matn –bu.. ====

#alifbo elementlarining tartiblangan to‘plami====

matnni shifrlash va shifrini ochish uchun kerakli axborot====

axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam====

kalit axborotni shifrlovchi kalitlar

++++

Masofadan ERI olish uchun qaysi internet manzilga murojaat qilinadi? ====

#e-imzo.uz====

elektron-imzo.uz====

imzo.uz====

eri.uz

++++

O‘rin almashtirish shifri bu - …====

#Murakkab bo‘lmagan kriptografik akslantirish====

Kalit asosida generatsiya qilish====

Ketma-ket ochiq matnni ustiga qo‘yish====

Belgilangan biror uzunliklarga bo‘lib chiqib shifrlash

++++

Parollash siyosatiga ko'ra parol tanlash shartlari qanday? ====

#Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. ====

Kamida 8 belgi; katta va kichik xavflar, sonlar qo'llanishi kerak.====

Kamida 6 belgi; katta xarflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak.====

Kamida 8 belgi; katta va kichik xavflar, sonlar qo'llanishi kerak.

++++

RSA algoritmi qanday jarayonlardan tashkil topgan? ====

#Kalitni generatsiyalash; Shifrlash; Deshifrlash. ====

Shifrlash; Imzoni tekshirish; Deshifrlash====

Kalitni generatsiyalash; imzolash; Deshifrlash. ====

Imzoni tekshirish ; Shifrlash; Deshifrlash.

++++

RSA qanday algoritm? ====

#Raqamli imzo algoritmi====

Shifrlash algoritmi====

Kalitli almashish algoritmi====

Shifrlash algoritmi va kalitli almashish algoritmi

++++

Shaxsning, o‘zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, axborot-kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu? ====

#login====

parol====

identifikatsiya====

maxfiy maydon

++++

Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi? ====

#Kriptobardoshlik====

Shifr matn uzunligi====

Shifrlash algoritmi====

Texnika va texnologiyalar

++++

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Savol** | **A** | **B** | **C** | **D** |
| Konfidensiallikni ta’minlash bu - ? | #ruxsatsiz o‘qishdan himoyalash. | ruxsatsiz yozishdan himoyalash. | ruxsatsiz bajarishdan himoyalash. | ruxsat etilgan amallarni bajarish. |
| Foydalanuvchanlikni ta’minlash bu - ? | ruxsatsiz yozishdan himoyalash. | #ruxsatsiz bajarishdan himoyalash. | ruxsatsiz o‘qishdan himoyalash. | ruxsat etilgan amallarni bajarish |
| Yaxlitlikni ta’minlash bu - ? | ruxsatsiz bajarishdan himoyalash. | ruxsatsiz o‘qishdan himoyalash. | #ruxsatsiz yozishdan himoyalash. | ruxsat etilgan amallarni bajarish |
| Jumlani to‘ldiring. Hujumchi kabi fikrlash ... kerak. | ma’lumotni aniq va ishonchli ekanligini bilish | kafolatlangan amallarni ta’minlash uchun | ma’lumot, axborot va tizimdan foydalanish uchun | #bo‘lishi mumkin bo‘lgan xavfni oldini olish uchun |
| Jumlani to‘ldiring. Tizimli fikrlash ... uchun kerak. | #kafolatlangan amallarni ta’minlash | bo‘lishi mumkin bo‘lgan xavfni oldini olish | ma’lumot, axborot va tizimdan foydalanish | ma’lumotni aniq va ishonchli ekanligini bilish |
| Axborot xavfsizligida risk bu - ? | Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa. | U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz. | #Manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta’sirida tahdid qilish ehtimoli. | bo‘lishi mumkin bo‘lgan xavfni oldini olish |
| Axborot xavfsizligida tahdid bu - ? | kafolatlangan amallarni ta’minlash uchun | Noaniqlikning maqsadlarga ta’siri. | U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz. | #Aktivga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
| Axborot xavfsizligida aktiv bu - ? | Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. | #Tashkilot yoki foydalanuvchi uchun qadrli bo‘lgan ixtiyoriy narsa. | Noaniqlikning maqsadlarga ta’siri | U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz. |
| Axborot xavfsizligida zaiflik bu - ? | Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. | Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa. | #Tahdidga sabab bo‘luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson. | Noaniqlikning maqsadlarga ta’siri. |
| Axborot xavfsizligida boshqarish vositasi bu - ? | Noaniqlikning maqsadlarga ta’siri. | Bir yoki bir nechta tahdidga sabab bo‘luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik. | Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa. | #Natijasi zaiflik yoki tahdidga ta’sir qiluvchi riskni o‘zgartiradigan harakatlar. |
| Har qanday vaziyatda biror bir hodisani yuzaga kelish ehtimoli qo‘shilsa ....... | yaxlitlik | hujum paydo bo‘ladi. | #risk paydo bo‘ladi. | butunlik |
| Jumlani to‘ldiring. Denial of service (DOS) hujumi axborotni .... xususiyatini buzushga qaratilgan. | #foydalanuvchanlik | butunlik | konfidensiallik | risk paydo bo‘ladi. |
| Jumlani to‘ldiring. ... sohasi tashkil etuvchilar xavfsizligi, aloqa xavfsizligi va dasturiy ta’minotlar xavfsizligidan iborat. | #Tizim xavfsizligi | Ma’lumotlar xavfsizligi | Inson xavfsizligi | Axborot xavfsizligi |
| Kriptologiya so‘ziga berilgan to‘g‘ri tavsifni toping - ? | #Maxfiy shifrlarni yaratish va buzish fani va sanati. | Maxfiy shifrlarni yaratish fani va sanati. | Maxfiy shifrlarni buzish fani va sanati. | Ochiq matn |
| .... kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi. | #Kriptografik kalit | Ochiq matn | Alifbo | Shifir matin |
| Kriptografiya so‘ziga berilgan to‘g‘ri tavsifni toping? | xesh funksiyalar. | Maxfiy shifrlarni yaratish va buzish fani va sanati. | Maxfiy shifrlarni buzish fani va sanati. | #Maxfiy shifrlarni yaratish fani va sanati. |
| Kriptotahlil so‘ziga berilgan to‘g‘ri tavsifni toping? | #Maxfiy shifrlarni buzish fani va sanati. | Maxfiy shifrlarni yaratish fani va sanati. | Maxfiy shifrlarni yaratish va buzish fani va sanati. | ochiq matn |
| ..... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to‘plami. | Ochiq matn | #Alifbo | Shifrmatn | Dishefirlash |
| Ma’lumot shifrlansa, natijasi .... bo‘ladi. | nomalum | ochiq matn | #shifrmatn | Alifbo |
| Deshifrlash uchun kalit va ..... kerak bo‘ladi. | #shifrmatn | ochiq matn | kodlash | alifbo |
| Ma’lumotni shifrlash va deshifrlashda yagona kalitdan foydalanuvchi tizim bu - | #simmetrik kriptotizim. | ochiq kalitli kriptotizim. | asimetrik kriptotizim. | xesh funksiyalar. |
| Ikki kalitli kriptotizim bu - | xesh funksiyalar. | simmetrik kriptotizim. | #ochiq kalitli kriptotizim. | MAC tizimlari. |
| Axborotni mavjudligini yashirish bilan shug‘ullanuvchi fan sohasi bu - | kriptotahlil. | kriptografiya. | kodlash. | #steganografiya. |
| Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ..... amalga oshiriladi. | #kodlash | shifrlash | yashirish | deshifrlash |
| Jumlani to‘ldiring. Ma’lumotni konfidensialligini ta’minlash uchun ..... zarur. | #shifrlash | kodlash | dekodlash | deshifrlash |
| Ma’lumotni mavjudligini yashirishda ..... | kriptotahlil algoritmidan foydalaniladi. | kriptografik algoritmdan foydalaniladi. | kodlash algoritmidan foydalaniladi. | #steganografik algoritmdan foydalaniladi. |
| Xesh funksiyalar - .... funksiya. | bir kalitli kriptografik algoritm | #kalitsiz kriptografik algoritm | ikki kalitli kriptografik algoritm | ko‘p kalitli kriptografik algoritm |
| Jumlani to‘ldiring. Ma’lumotni uzatishda kriptografik himoya ..... | foydalanuvchanlik va butunlikni ta’minlaydi. | konfidensiallik va foydalanuvchanlikni ta’minlaydi. | #konfidensiallik va butunlikni ta’minlaydi. | konfidensiallik ta’minlaydi. |
| Jumlani to‘ldiring. ... kompyuter davriga tegishli shifrlarga misol bo‘la oladi. | Kodlar kitobi | Sezar shifri | #DES, AES shifri | Enigma shifri |
| .... kriptografik shifrlash algoritmlari blokli va oqimli turlarga ajratiladi. | #Simmetrik | Ochiq kalitli | Asimmetrik | Klassik davr |
| Kiberjinoyatchilik bu - ? | #Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. | Kompyuterlar bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta’sir ko‘rsatishini o‘rganadi. | Hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. | Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti. |
| Kiberetika bu - ? | Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti. | Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. | Hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. | #Kompyuterlar bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta’sir ko‘rsatishini o‘rganadi. |
| Qanday tahdidlar passiv hisoblanadi? | Texnik vositalar bilan bog‘liq bo‘lgan tahdidlar | Hech qachon amalga oshirilmaydigan tahdidlar | Axborot xavfsizligini buzmaydigan tahdidlar | #Amalga oshishida axborot strukturasi va mazmunida hech narsani o‘zgartirmaydigan tahdidlar |
| Quyidagi qaysi hujum turi razvedka hujumlari turiga kirmaydi? | Ping buyrug‘ini yuborish | Paketlarni snifferlash | Portlarni skanerlash | #Ddos |
| Quyidagilarnnig qaysi biri tabiiy tahdidlarga misol bo’la oladi? | O’g’irlik, toshqinlar, zilzila | Bosqinchilik, terrorizm, o‘g‘irlik | #Toshqinlar, yong’in, zilzila | Terorizim, toshqinlar, zilzila |
| Quyidagilarnnig qaysi biri sun’iy tahdidlarga misol bo’la oladi? | Toshqinlar, zilzila, toshqinlar | #Bosqinchilik, terrorizm, o‘g‘irlik | O’g’irlik, toshqinlar, zilzila | Terorizim, toshqinlar, zilzila |
| Kolliziya hodisasi deb nimaga aytiladi? | ikki xil matn uchun ikki xil xesh qiymat chiqishi | #ikki xil matn uchun bir xil xesh qiymat chiqishi | bir xil matn uchun bir xil xesh qiymat chiqishi | bir xil matn uchun ikki xil xesh qiymat chiqishi |
| GSM tarmog‘ida foydanalaniluvchi shifrlash algoritmi nomini ko‘rsating? | RC4 | DES | AES | #A5/1 |
| O‘zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko‘rsating? | Kadastr agentligi | “O‘zstandart” agentligi | Davlat Soliq Qo‘mitasi | #“UNICON.UZ” DUK |
| Simmetrik kriptotizimlarda necha kalitdan foydalaniladi? | #1 ta | 3 ta | 4 ta | kalit ishlatilmaydi |
| Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting? | #Doimo xavfsiz saqlab olib yurish zaruriyati. | Doimo esada saqlash zaruriyati. | Qalbakilashtirish muammosi mavjudligi. | Almashtirib bo‘lmaslik. |
| Esda saqlashni va olib yurishni talab etmaydigan autentifikatsiya usuli bu - | ko‘p faktorli autentifikatsiya. | parolga asoslangan autentifikatsiya. | tokenga asoslangan autentifikatsiya. | #biometrik autentifikatsiya. |
| Qaysi biometrik parametr eng yuqori universallik xususiyatiga ega? | Qo‘l shakli. | Ko‘z qorachig‘i. | Barmoq izi. | #Yuz tasviri. |
| Qaysi biometrik parametr eng yuqori takrorlanmaslik xususiyatiga ega? | Yuz tasviri. | #Ko‘z qorachig‘i. | Barmoq izi. | Qo‘l shakli. |
| Quyidagilardan qaysi biri har ikkala tomonning haqiqiyligini tekshirish jarayonini ifodalaydi? | Ikki faktorli autentifikatsiya. | #Ikki tomonlama autentifikatsiya. | Ko‘p faktorli autentifikatsiya. | Biometrik autentifikatsiya. |
| Foydalanuvchi parollari bazada qanday ko‘rinishda saqlanadi? | #Xeshlangan ko‘rinishda. | Shifrlangan ko‘rinishda. | Ochiq holatda. | Bazada saqlanmaydi. |
| Quyidagilardan qaysi biri tabiy tahdidga misol bo‘ladi? | #Yong‘in, suv toshishi, harorat ortishi. | Yong‘in, o‘g‘irlik, qisqa tutashuvlar. | Suv toshishi, namlikni ortib ketishi, bosqinchilik. | Bosqinchilik, terrorizm, o‘g‘irlik. |
| Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan? | #Ma’muriy nazoratlash. | Fizik nazoratlash. | Texnik nazoratlash. | Apparat nazoratlash. |
| OSI tarmoq modeli nechta sathdan iborat? | 4 | #7 | 6 | 5 |
| TCP/IP tarmoq modeli nechta sathdan iborat? | #4 | 7 | 6 | 5 |
| Hajmi bo‘yicha eng kichik hisoblangan tarmoq turi bu - | #PAN | LAN | CAN | MAN |
| Razvedka hujumlari bu? | Tizimni fizik buzishni maqsad qiladi. | Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. | Foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi. | #Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi. |
| Kirish hujumlari bu? | Foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi. | Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi. | Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. | Tarmoq haqida axborotni to‘plash hujumchilarga mavjud bo‘lgan potensial zaiflikni aniqlashga harakat qiladi. |
| Paketlarni snifferlash, portlarni skanerlash va Ping buyrug‘ini yuborish hujumlari qaysi hujumlar toifasiga kiradi? | DOS hujumlari. | Kirish hujumlari. | #Razvedka hujumlari. | Zararli dasturlar yordamida amalga oshiriladigan hujumlar. |
| O‘zini yaxshi va foydali dasturiy vosita sifatida ko‘rsatuvchi zararli dastur turi bu? | Backdoors. | Adware. | Spyware. | #Troyan otlari. |
| Himoya mexanizmini aylanib o‘tib tizimga ruxsatsiz kirish imkonini beruvchi zararli dastur turi bu? | #Backdoors. | Adware. | Troyan otlari. | Spyware. |
| Eng zaif simsiz tarmoq protokolini ko‘rsating? | #WEP | WPA | WPA2 | WPA3 |
| Axborotni shifrlashdan maqsadi nima? | Malumotlarni yig‘ish va sotish. | Ma’lumotlarni zichlashtirish, siqish. | #Maxfiy xabar mazmunini yashirish. | Ma’lumotlarni uzatish. |
| Virus aniq bo‘lganda va xususiyatlari aniq ajratilgan holatda eng katta samaradorlikka ega zararli dasturni aniqlash usulini ko‘rsating? | O‘zgarishga asoslangan usul | #Signaturaga asoslangan usul | Anomaliyaga asoslangan usul | Barcha javoblar to‘g‘ri |
| Zararli dasturiy vositalarga qarshi foydalaniluvchi dasturiy vosita bu? | Brandmauer | VPN | Tarmoqlararo ekran | #Antivirus |
| Kompyuter viruslarini tarqalish usullarini ko‘rsating? | #Ma’lumot saqlovchilari, Internetdan yuklab olish va elektron pochta orqali. | Ma’lumot saqlovchilari, Internetdan yuklab olish va skaner qurilmalari orqali. | Printer qurilmasi, Internetdan yuklab olish va elektron pochta orqali. | Barcha javoblar to‘g‘ri. |
| Biror mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu-? | #Mantiqiy bombalar. | Backdoors. | Adware. | Virus. |
| Ma’lumotni to‘liq qayta tiklash qachon samarali amalga oshiriladi? | Ma’lumotni o‘chirish Shifr+Delete buyrug‘i bilan amalga oshirilgan bo‘lsa. | Ma’lumotni o‘chirish Delete buyrug‘i bilan amalga oshirilgan bo‘lsa. | #Saqlagichda ma’lumot qayta yozilmagan bo‘lsa. | Formatlash asosida ma’lumot o‘chirilgan bo‘lsa. |
| Jumlani to‘ldiring. ... texnologiyasi lokal simsiz tarmoqlarga tegishli. | #WI-FI | WI-MAX | GSM | Bluetooth |
| Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga imkon beruvchi himoya vositasi bu? | #Tarmoqlararo ekran. | Virtual Private Network. | Antivirus. | Router. |
| Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi- bu qanday hujum turi? | Zararli hujumlar | Kirish hujumlari | Dos hujumlari | #Razvedka hujumlari |
| Biror axborotni o‘g‘irlanishiga yoki yo‘qolishiga olib kelmasada, biroq tashkilot funksiyasini bajarilmasligiga olib keladi - bu qanday hujum turi? | Razvedka hujumlari | Kirish hujumlari | Dos hujumlari | #Zararli hujumlar |
| Tarmoq sathidagi VPN qaysi protokol asosida quriladi? | PPTP | TLS | L2F | #IPSec |
| Tashkilotda ma’lumotlarni yo’q qilishda kesish orqali yo’q qilish usuli qaysi? | #maydalash | yoqish | ko’mish | kimyoviy ishlov berish |
| Risk bu - ? | #Belgilangan sharoitlarda tahdidning manbalarga potentsial zarar etkazilishini kutish | Foydalanuvchining ro’yxatdan o’tgandan keyingi jarayoni | Zaifliklarni tadqiq qilish va ularni bartaraf etuvchi nazoratni  aniqlash | Nazoratni amalga oshirish orqali tahdid yoki zaiflik bilan aloqador risklarni kamaytirish |
| Riskni kamaytirish –? | #Nazoratni amalga oshirish orqali tahdid yoki zaiflik bilan aloqador risklarni kamaytirish | АT xavfsizlik dasturi boshligʼi: tashkilot axborot xavfsizligi dasturi uchun javobgarlik | Avtomatlashtirilgan identifikatsiyalash to’plami | Vositalarini aniqlash va oʼrnatish |
| … – zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat. Nuqtalar o’rniga kerakli javobni tanlang. | Tahdid | #Hujum | Zaiflik | Xavf- xatar |
| Bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi. Bu qanday zararkunanda dastur? | Viruslar | #Troyan otlari | Adware | Spyware |
| Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot. Bu qanday zararkunanda dastur? | Spyware | Viruslar | Troyan otlari | #Adware |
| Foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod. Bu qanday zararkunanda dastur? | Troyan otlari | Viruslar | #Spyware | Adware |
| Zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish. | #Backdoors | Rootkits | Mantiqiy bombalar | Botnet |
| Zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi. | A)Mantiqiy bombalar | Rootkits | Backdoors | Botnet |
| Mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi. | Rootkits | Mantiqiy bombalar | Backdoors | #Ransomware |
| Qaysi vosita tashqi tapmoqdagi foydalanuvchilapdan ichki tarmoq resurslarini himoyalash vazifasini bajarmaydi? | Tarmoklararo ekran | Braundmauer | Firewall | #Antivirus |
| Qaysi vosita ichki tarmok foydalanuvchilapini tashqi tarmoqqa bo‘lgan murojaatlarini chegaralash vazifasini bajaradi? | Antivirus | #Braundmauer | Vpn | IDS |
| Biba modeli axborotni qaysi xususiyatini ta’minlashni maqsad qiladi? | #Butunlik | Konfidensiallik | Foydalanuvchanlik | Maxfiylik |
| Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi? | #Apparat | Dasturiy | Simmetrik | Ochiq kalitli |
| 64 ta belgidan iborat Sezar shifrlash usilida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin? | #63 | 63! | 32 | 322 |
| “Yelka orqali qarash” hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan. | #Parolga asoslangan autentifikatsiya | Tokenga asoslangan autentifikatsiya | Biometrik autentifikatsiya | Ko‘z qorachig‘iga asoslangan autentifikatsiya |
| Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan | #Parolga asoslangan autentifikatsiya | #Parolga  asoslangan autentifikatsiya | Biometrik autentifikatsiya | Ko‘z qorachig‘iga asoslangan autentifikatsiya |
| Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan | #Biometrik autentifikatsiya | Biror narsani bilishga asoslangan autentifikatsiya | Biror narsaga egalik qilishga asoslangan autentifikatsiya | Tokenga asoslangan autentifikatsiya |
| Axborotni butunligini ta’minlash usullarini ko‘rsating | #Xesh funksiyalar, MAC | Shifrlash usullari | Assimetrik shifrlash usullari, CRC tizimlari | Shifrlash usullari, CRC tizimlari |

KIBERXAVSIZLIK JAVOBLARI ORALIQ

1.#Konfidensiallikni ta'minlash bu - ?   
+ruxsatsiz o'qishdan himoyalash.   
2.#Foydalanuvchanlikni ta'minlash bu - ?   
+ruxsatsiz bajarishdan himoyalash.   
3.#Yaxlitlikni ta'minlash bu - ?   
+ruxsatsiz yozishdan himoyalash.   
4.#Jumlani to'ldiring. Hujumchi kabi fikrlash ... kerak.   
+bo'lishi mumkin bo'lgan [xavfni oldini olish uchun](https://fayllar.org/1-oquvchilar-nutqidagi-xatoliklarni-aniqlash-va-bartaraf-etish.html)   
5.#Jumlani to'ldiring. Tizimli fikrlash ... uchun kerak.   
+kafolatlangan amallarni ta'minlash   
6.#Axborot xavfsizligida risk bu?   
+Manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta'sirida tahdid qilish ehtimoli.   
7.#Axborot xavfsizligida tahdid bu?   
+Aktivga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.   
8.#Axborot xavfsizligida aktiv bu?   
+Tashkilot yoki foydalanuvchi uchun qadrli bo'lgan ixtiyoriy narsa.   
9.#Axborot xavfsizligida zaiflik bu?   
+Tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson.   
10.#Axborot xavfsizligida boshqarish vositasi bu?   
+Natijasi zaiflik yoki tahdidga ta'sir qiluvchi riskni o'zgartiradigan harakatlar.   
11.#Har qanday vaziyatda biror bir hodisani yuzaga kelish ehtimoli qo'shilsa ....   
+risk paydo bo'ladi.   
12.#Jumlani to'ldiring. Denial of service (DOS) hujumi axborotni .... xususiyatini buzushga qaratilgan.   
+foydalanuvchanlik   
13.#Jumlani to'ldiring. ... sohasi tashkil etuvchilar xavfsizligi, aloqa xavfsizligi va dasturiy ta'minotlar xavfsizligidan iborat.   
+Tizim xavfsizligi   
14.#Kriptologiya so'ziga berilgan to'g'ri tavsifni toping?   
+Maxfiy shifrlarni yaratish va buzish fani va sanati.   
15.#.... kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi.   
+Kriptografik kalit   
16.#Kriptografiya so'ziga berilgan to'g'ri tavsifni toping?   
+Maxfiy shifrlarni yaratish fani va sanati.   
17.#Kriptotahlil so'ziga berilgan to'g'ri tavsifni toping?   
+Maxfiy shifrlarni buzish fani va sanati.   
18.#..... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to'plami.   
+Alifbo   
19.#Ma'lumot shifrlansa, natijasi .... bo'ladi.   
+shifrmatn   
20.#Deshifrlash uchun kalit va ..... kerak bo'ladi.   
+shifrmatn   
21.#Ma'lumotni shifrlash va deshifrlashda yagona kalitdan foydalanuvchi tizim bu -   
+simmetrik kriptotizim.   
22.#Ikki kalitli kriptotizim bu -   
+ochiq kalitli kriptotizim.   
23.#Axborotni mavjudligini yashirish bilan shug'ullanuvchi fan sohasi bu -   
+steganografiya.   
24.#Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ..... amalga oshiriladi.   
+kodlash   
25.#Jumlani to'ldiring. Ma'lumotni konfidensialligini ta'minlash uchun ..... zarur.   
+shifrlash   
26.#Ma'lumotni mavjudligini yashirishda .....   
+steganografik algoritmdan foydalaniladi.   
27.#Xesh funksiyalar - .... funksiya.   
+kalitsiz [kriptografik](https://fayllar.org/reja-i-kirish-ii-asosiy-qism-jeferson-kriptografik-shifrlash-q.html)   
28.#Jumlani to'ldiring. Ma'lumotni uzatishda kriptografik himoya .....   
+konfidensiallik va butunlikni ta'minlaydi.   
29.#Jumlani to'ldiring. ... kompyuter davriga tegishli shifrlarga misol bo'la oladi.   
+DES, AES shifri   
30.#.... kriptografik shifrlash algoritmlari blokli va oqimli turlarga ajratiladi.   
+Simmetrik   
31.#Jumlani to'ldiring. .... shifrlar tasodifiy ketma-ketliklarni generatsiyalashga asoslanadi.   
+Oqimli   
32.#Ochiq matn qismlarini takroriy shifrlovchi algoritmlar bu -   
+blokli shifrlar   
33#A5/1 shifri bu -   
+oqimli shifr.   
34.#Quyidagi muammolardan qaysi biri simmetrik kriptotizimlarga xos.   
+Kalitni taqsimlash zaruriyati.   
35.#Quyidagi atamalardan qaysi biri faqat simmetrik blokli shifrlarga xos?   
+Blok uzunligi.   
36.#Jumlani to'ldiring. Sezar shifri .... akslantirishga asoslangan.   
+o'rniga qo'yish   
37.#Kriptotizimning to'liq xavfsiz bo'lishi Kerxgofs prinsipiga ko'ra qaysi kattalikning nomalum bo'lishiga asoslanadi?   
+Kalit.   
38.#Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi shifrlar bu -   
+ochiq kalitli shifrlar.   
39.#Agar simmetrik kalitning uzunligi 64 bit bo'lsa, jami bo'lishi mumkin bo'lgan kalitlar soni nechta?   
+264   
40.#Axborotni qaysi xususiyatlari simmetrik shifrlar yordamida ta'minlanadi.   
+Konfidensiallik va butunlik.   
41.#Axborotni qaysi xususiyatlari ochiq kalitli shifrlar yordamida ta'minlanadi.   
+Konfidensiallik.   
42.#Elektron raqamli imzo tizimi.   
+MAC tizimlari.   
43.#Qaysi ochiq kalitli algoritm katta sonni faktorlash muammosiga asoslanadi?   
+RSA algoritmi.   
44.#Rad etishdan himoyalashda ochiq kalitli kriptotizimlarning qaysi xususiyati muhim hisoblanadi.   
+Ikkita kalitdan foydalanilgani.   
45.#Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas.   
+Bir tomonlama funksiya bo'lmasligi kerak.   
46.#Quyidagi xususiyatlardan qaysi biri elektron raqamli imzo tomonidan ta'minlanadi?   
+Axborot butunligini va rad etishdan himoyalash.   
47.#Faqat ma'lumotni butunligini ta'minlovchi kriptotizimlarni ko'rsating.   
+MAC (Xabarlarni autentifikatsiya kodlari) tizimlari.   
48.#Foydalanuvchini tizimga tanitish jarayoni bu?   
+Identifikatsiya.   
49.Foydalanuvchini haqiqiyligini tekshirish jarayoni bu?   
+Autentifikatsiya.   
50.Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu?   
+Avtorizatsiya.   
51.Parolga asoslangan autentifikatsiya usulining asosiy kamchiligini ko'rsating?   
+Esda saqlash zaruriyati.   
52.Biror narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilar tushuniladi.   
+PIN, Parol.   
53.Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting?   
+Doimo xavfsiz saqlab olib yurish zaruriyati.   
54.Esda saqlashni va olib yurishni talab etmaydigan autentifikatsiya usuli bu -   
+biometrik autentifikatsiya.   
55.Qaysi biometrik parametr eng yuqori universallik xususiyatiga ega?   
+Yuz tasviri.   
56.Qaysi biometrik parametr eng yuqori takrorlanmaslik xususiyatiga ega?   
+Ko'z qorachig'i.   
57.Quyidagilardan qaysi biri har ikkala tomonning haqiqiyligini tekshirish jarayonini ifodalaydi?   
+Ikki tomonlama autentifikatsiya.   
58.Parolga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating?   
+Parollar lug'atidan [foydalanish asosida hujum](https://fayllar.org/universitetining-jizzax-filiali-psixologiya-fakulteti-psixolog-v5.html), yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum.   
59.Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating?   
+Fizik o'g'irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar   
60.Foydalanuvchi parollari bazada qanday ko'rinishda saqlanadi?   
+Xeshlangan ko'rinishda.   
61.Agar parolning uzunligi 8 ta belgi va har bir o'rinda 128 ta turlicha belgidan foydalanish mumkin bo'lsa, bo'lishi mumkin bo'lgan jami parollar sonini toping.   
+1288   
62.Parolni "salt" (tuz) kattaligidan foydalanib xeshlashdan (h(password, salt)) asosiy maqsad nima?   
+Buzg'unchiga ortiqcha hisoblashni talab etuvchi murakkablikni yaratish.   
63.Quyidagilardan qaysi biri tabiy tahdidga misol bo'ladi?   
+Yong'in, suv toshishi, harorat ortishi.   
64.Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan?   
+Ma'muriy nazoratlash.   
65.Faqat ob'ektning egasi tomonidan foydalanishga mos bo'lgan mantiqiy foydalanish usulini ko'rsating?   
+Diskretsion foydalanishni boshqarish.   
66.Qaysi usul ob'ektlar va sub'ektlarni klassifikatsiyalashga asoslangan?   
+Mandatli foydalanishni boshqarish.   
67.Biror faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami bu?   
+Rol.   
68.Qoida, siyosat, qoida va siyosatni mujassamlashtirgan algoritmlar, majburiyatlar va maslahatlar kabi tushunchalar qaysi foydalanishni boshqarish usuliga aloqador.   
+Attributga asoslangan foydalanishni boshqarish.   
69Bell-Lapadula modeli axborotni qaysi xususiyatini ta'minlashni maqsad qiladi?   
+Konfidensiallik.   
70.Biba modeli axborotni qaysi xususiyatini ta'minlashni maqsad qiladi?   
+Butunlik.   
71.Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi?   
+Apparat.   
72.Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalanadi?   
+Dasturiy.   
73.Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko'rsating?   
+Ochiq kalitli shifrlar.   
74.Xesh funksiyalarda kolliziya hodisasi bu?   
+Ikki turli matnlarning xesh qiymatlarini bir xil bo'lishi.   
75.64 ta belgidan iborat Sezar shifrlash usilida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin?   
+63   
76.Elektron raqamli imzo muolajalarini ko'rsating?   
+Imzoni shakllantirish va imkoni tekshirish.   
77."Yelka orqali qarash" hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.   
+Parolga asoslangan autentifikatsiya.   
78.Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan.   
+Parolga asoslangan autentifikatsiya.   
79.Yo'qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon.   
+Parolga asoslangan autentifikatsiya.   
80.Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.   
+Biometrik autentifikatsiya.   
81,Axborotni butunligini ta'minlash usullarini ko'rsating.   
+Xesh funksiyalar, MAC.   
82.#Quyidagilardan qaysi biri to'liq kompyuter topologiyalarini ifodalamaydi.   
+LAN, GAN, OSI.   
83.#OSI tarmoq modeli nechta sathdan iborat?   
+7   
84.#TCP/IP tarmoq modeli nechta sathdan iborat?   
+4   
85.#Hajmi bo'yicha eng kichik hisoblangan tarmoq turi bu -   
+PAN   
86.#IPv6 protokolida IP manzilni ifodalashda necha bit ajratiladi.   
+128   
87.#IP manzilni domen nomlariga yoki aksincha almashtirishni [amalga oshiruvchi xizmat bu-](https://fayllar.org/mantiqiy-element-kirish-va-chiqish-boyicha-va-signal-sathlarin.html)   
+DNS   
88.#Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi hodisalarning potensial paydo bo'lishi bu?   
+Tahdid.   
89.#Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat bu?   
+Hujum.   
90.#Quyidagilardan qaysi biri tarmoq xavfsizligi muammolariga sabab bo'lmaydi?   
+Routerlardan foydalanmaslik.   
91.#Tarmoq xavfsizligini buzulishi biznes faoliyatga qanday ta'sir qiladi?   
+Biznes faoliyatning buzilishi, huquqiy javobgarlikka sababchi bo'ladi.   
92.#Razvedka hujumlari bu?   
+Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi.   
93.#Kirish hujumlari bu?   
+Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.   
94.#Xizmatdan vos kechishga qaratilgan hujumlar bu?   
+Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.   
95.#Paketlarni snifferlash, portlarni skanerlash va Ping buyrug'ini yuborish hujumlari qaysi hujumlar toifasiga kiradi?   
+Razvedka hujumlari.   
96.#O'zini yaxshi va foydali dasturiy vosita sifatida ko'rsatuvchi zararli dastur turi bu?   
+Troyan otlari.   
97.#Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi zararli dastur turi bu?   
+Adware.   
98.#Himoya mexanizmini aylanib o'tib tizimga ruxsatsiz kirish imkonini beruvchi zararli dastur turi bu?   
+Backdoors.   
99.#Paket filterlari turidagi tarmoqlararo ekran vositasi OSI modelining qaysi sathida ishlaydi?   
+Tarmoq sathida.   
100.#Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi.   
+Tarmoqlararo ekran.   
101.Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo'lgan murojaatlarini chegaralash qaysi himoya vositasining vazifasi hisoblanadi.   
+Tarmoqlararo ekran.   
102.2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo'yicha qo'shing?   
+00001   
103.2 lik sanoq tizimida 11011 soniga 00100 sonini 2 modul bo'yicha qo'shing?   
+11111   
104.2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo'yicha qo'shing?   
+00001   
105.Axborot saqlagich vositalaridan qayta foydalanish xususiyatini saqlab qolgan holda axborotni yo'q qilish usuli qaysi?   
+Bir necha marta takroran yozish va maxsus dasturlar yordamida saqlagichni tozalash   
106.Elektron ma'lumotlarni yo'q qilishda maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o'zgartiriladigan usul bu ...   
+magnitsizlantirish.   
107.Yo'q qilish usullari orasidan ekologik jihatdan ma'qullanmaydigan va maxsus joy talab qiladigan usul qaysi?   
+Yoqish   
108.Kiberjinoyatchilik bu - ?   
+Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.   
109.Kiberetika bu - ?   
+Kompyuterlar bilan bog'liq falsafiy soha bo'lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko'rsatishini o'rganadi.   
110.Shaxsiy simsiz tarmoqlar qo'llanish sohasini belgilang   
+Tashqi qurilmalar kabellarining o'rnida   
111.VPNning texnik yechim arxitekturasiga ko'ra turlari keltirilgan qatorni aniqlang?   
+Korporativ tarmoq ichidagi VPN; [masofadan foydalaniluvchi VPN](https://fayllar.org/masofadan-kompyuterlarni-boshqarish.html); korporativ tarmoqlararo VPN   
112.Axborotning konfidensialligi va butunligini ta'minlash uchun ikki uzel orasida himoyalangan tunelni quruvchi himoya vositasi bu?   
+Virtual Private Network   
113.Qanday tahdidlar passiv hisoblanadi?   
+Amalga oshishida axborot strukturasi va mazmunida hech narsani o'zgartirmaydigan tahdidlar   
114Quyidagi qaysi hujum turi razvedka hujumlari turiga kirmaydi?   
+Ddos   
115.Trafik orqali axborotni to'plashga harakat qilish razvedka hujumlarining qaysi turida amalga oshiriladi?   
+Passiv   
116.Portlarni va operatsion tizimni skanerlash razvedka hujumlarining qaysi turida amalga oshiriladi?   
+Aktiv   
117.Paketlarni snifferlash, portlarni skanerlash, ping buyrug'ini yuborish qanday hujum turiga misol bo'ladi?   
+Razvedka hujumlari   
118.DNS serverlari tarmoqda qanday vazifani amalga oshiradi?   
+Xost nomlari va internet nomlarini IP manzillarga o'zgartirish va [teskarisini amalga oshiradi](https://fayllar.org/majburiy-sertifikatlashtirish-talablariga-rioya-etilishi-ustid.html)   
119.Markaziy xab yoki tugun orqali tarmoqni markazlashgan holda boshqarish qaysi tarmoq topologiyasida amalga oshiriladi?   
+Yulduz   
120.Quyidagilardan qaysilari ananaviy tarmoq turi hisoblanadi?   
+WAN, MAN, LAN   
121.Quyidagilardan qaysilari tarmoq topologiyalari hisoblanadi?   
+Halqa, yulduz, shina, daraxt   
122.Yong'inga qarshi tizimlarni aktiv chora turiga quyidagilardan qaysilari kiradi?   
+Yong'inni aniqlash va bartaraf etish tizimi   
123.Yong'inga qarshi kurashishning aktiv usuli to'g'ri ko'rsatilgan javobni toping?   
+Tutunni aniqlovchilar, alangani aniqlovchilar va issiqlikni aniqlovchilar   
124.Yong'inga qarshi kurashishning passiv usuliga kiruvchi choralarni to'g'ri ko'rsatilgan javobni toping?   
+Minimal darajada yonuvchan materiallardan foydalanish, qo'shimcha etaj va xonalar qurish   
125.Fizik himoyani buzilishiga olib keluvchi tahdidlar yuzaga kelish shakliga ko'ra qanday guruhlarga bo'linadi?   
+Tabiy va sun'iy   
126.Quyidagilarnnig qaysi biri tabiiy tahdidlarga misol bo'la oladi?   
+Toshqinlar, yong'in, [zilzila](https://fayllar.org/mavzu-zilzila-va-uning-turlari-seysmik-tumanlarda-qurilish-ish.html)   
127.Quyidagilarnnig qaysi biri sun'iy tahdidlarga misol bo'la oladi?   
+Bosqinchilik, terrorizm, o'g'irlik   
128.Kolliziya hodisasi deb nimaga aytiladi?   
+Ikki xil matn uchun bir xil xesh qiymat chiqishi   
129.GSM tarmog'ida foydanalaniluvchi shifrlash algoritmi nomini ko'rsating?   
+A5/1   
130.O'zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko'rsating?   
+"UNICON.UZ" DUK   
131.RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?   
+1   
132.A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?   
+1   
133.AES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?   
+1   
134.DES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?   
+1   
135.A5/1 oqimli shifrlash algoritmida maxfiy kalit necha registrga bo'linadi?   
+3   
136.Faqat simmetrik blokli shifrlarga xos bo'lgan atamani aniqlang?   
+blok uzunligi   
137.A5/1 shifri qaysi turga mansub?   
+oqimli shifrlar   
138…..shifrlar blokli va oqimli turlarga ajratiladi   
+simmetrik   
139.Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?   
+ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'lmaydi   
140.Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?   
+chiqishda fiksirlangan uzunlikdagi qiymatni beradi   
141.Xesh qiymatlarni yana qanday atash mumkin?   
+dayjest   
142.A5/1 oqimli shifrlash algoritmida dastlabki kalit uzunligi nechi bitga teng?   
+64   
143.A5/1 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi?   
+mobil aloqa [standarti GSM protokolida](https://fayllar.org/va-kummunikatsiyalarini-rivojlantirish-vazirligi-muhammad-al-x-v7.html)   
144.Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?   
+2 ta   
145.Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?   
+1 ta   
146.Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi?   
+simmetrik va assimetrik turlarga   
147.Kriptologiya qanday yo'nalishlarga bo'linadi?   
+kriptografiya va kriptotahlil   
148.Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?   
+Barcha javoblar to'g'ri   
149.Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating?   
+Paydo bo'layotgan zararli dasturiy vositalar sonining ko'pligi.   
150…..umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi.   
+Tarmoqlararo ekran   
151.RSA algoritmida p=5, q=13, e=7 ga teng bo'lsa, shaxsiy kalitni hisoblang?   
+7   
152….hujumida hujumchi o'rnatilgan aloqaga suqilib kiradi va aloqani bo'ladi. Nuqtalar o'rniga mos javobni qo'ying.   
+O'rtada turgan odam.   
153.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.   
+MAC   
154.GSM tarmog'ida ovozli so'zlashuvlarni shifrlash algoritmi bu?   
+A5/1   
155.RSA algoritmida ochiq kalit e=7, N=35 ga teng bo'lsa, M=2 ga teng ochiq matnni shifrlash natijasini ko'rsating?   
+23   
156.RSA algoritmida ochiq kalit e=7, N=143 ga teng bo'lsa, M=2 ga teng ochiq matnni shifrlash natijasini ko'rsating?   
+128   
157.Jumlani to'ldiring. Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishiga olib kelsa.   
+jinoyat sifatida baholanadi.   
158.Jumlani to'ldiring. Simli va simsiz tarmoqlar orasidagi asosiy farq ...   
+tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud mavjudigi.   
159.Jumlani to'ldiring. Simmetrik shifrlash algoritmlari ochiq ma'lumotdan foydalanish tartibiga ko'ra ...   
+blokli va oqimli turlarga bo'linadi.   
160.Jumlani to'ldiring. Tarmoqlararo ekranning vazifasi ...   
+ishonchli va ishonchsiz tarmoqlar orasida ma'lumotlarga kirishni boshqarish.   
161.Faktorlash muammosi asosida yaratilgan assimetrik shifrlash usuli?   
+RSA   
162.Eng zaif simsiz tarmoq protokolini ko'rsating?   
+WEP   
163.Axborotni shifrlashdan maqsadi nima?   
+Maxfiy xabar mazmunini yashirish.   
164. 9 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?   
+10, 8   
165. 12 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?   
+11, 13   
166. 13 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?   
+5, 7   
167.Jumlani to'ldiring. Autentifikatsiya tizimlari asoslanishiga ko'ra ... turga bo'linadi.   
+3   
168. ….umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi.   
+Tarmoqlararo ekran   
169. Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating?   
+Paydo bo'layotgan zararli dasturiy vositalar sonining ko'pligi.   
170.Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?   
+Barcha javoblar to'g'ri   
171.Virus aniq bo'lganda va xususiyatlari aniq ajratilgan holatda eng katta samaradorlikka ega zararli dasturni aniqlash usulini ko'rsating?   
+Signaturaga asoslangan usul   
172.Signatura (antiviruslarga aloqador bo'lgan) bu-?   
+Fayldan topilgan bitlar qatori.   
173.Zararli dasturiy vositalarga qarshi foydalaniluvchi dasturiy vosita bu?   
+Antivirus   
174.Kompyuter viruslarini tarqalish usullarini ko'rsating?   
+Ma'lumot saqlovchilari, Internetdan yuklab olish va elektron pochta orqali.   
175.Qurbon kompyuteridagi ma'lumotni shifrlab, uni deshifrlash uchun to'lovni amalga oshirishni talab qiluvchi zararli dastur bu-?   
+Ransomware.   
176.Internet tarmog'idagi obro'sizlantirilgan kompyuterlar bu-?   
+Botnet.   
178.Biror mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu-?   
+Mantiqiy bombalar.   
179.Buzg'unchiga xavfsizlik tizimini aylanib o'tib tizimga kirish imkonini beruvchi zararli dastur turi bu-?   
+Backdoors.   
180.Ma'lumotni to'liq qayta tiklash qachon samarali amalga oshiriladi?   
+Saqlagichda ma'lumot qayta yozilmagan bo'lsa.   
181.Ma'lumotni zaxira nusxalash nima uchun potensial tahdidlarni paydo bo'lish ehtimolini oshiradi.   
+Tahdidchi uchun nishon ko'payadi.   
182.Qaysi xususiyatlar RAID texnologiyasiga xos emas?   
+Shaxsiy kompyuterda foydalanish mumkin.   
183.Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo'shimcha apparat va dasturiy vositani talab qiladi?   
+Lentali disklar.   
184.Ma'lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi?   
+Zarur axborotni tanlashdan.   
185.Jumlani to'ldiring. .... - muhim bo'lgan axborot nusxalash yoki saqlash jarayoni bo'lib, bu ma'lumot yo'qolgan vaqtda qayta tiklash imkoniyatini beradi.   
+Ma'lumotlarni zaxira nusxalash   
186.Paket filteri turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi?   
+Tarmoq sathi parametrlari asosida.   
187.Jumlani to'ldiring. ... texnologiyasi lokal simsiz tarmoqlarga tegishli.   
+WI-FI   
188.Jumlani to'ldiring. Kriptografik himoya axborotning ... xususiyatini ta'minlamaydi.   
+Foydalanuvchanlik   
189.Jumlani to'ldiring. Parol kalitdan .... farq qiladi.   
+tasodifiylik [darajasi bilan](https://fayllar.org/17-metallarda-fermi-darajasi-va-fermi-dirak-taqsimot-funksiyas.html)   
190.Parolga "tuz"ni qo'shib xeshlashdan maqsad?   
+Tahdidchi ishini oshirish.   
191.Axborotni foydalanuvchanligini buzishga qaratilgan tahdidlar bu?   
+DDOS tahdidlar.   
192.Tasodifiy tahdidlarni ko'rsating?   
+Texnik vositalarning buzilishi va ishlamasligi.   
193.Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga imkon beruvchi himoya vositasi bu?   
+Tarmoqlararo ekran.   
194.Qaysi himoya vositasi yetkazilgan axborotning butunligini tekshiradi?   
+Virtual Private Network.   
195.Qaysi himoya vositasi tomonlarni autentifikatsiyalash imkoniyatini beradi?   
+Virtual Private Network.   
196.Foydalanuvchi tomonidan kiritilgan taqiqlangan so'rovni qaysi himoya vositasi yordamida nazoratlash mumkin.   
+Tarmoqlararo ekran.   
197.Qaysi himoya vositasi mavjud IP - paketni to'liq shifrlab, unga yangi IP sarlavha beradi?   
+Virtual Private Network.   
198,Ochiq tarmoq yordamida himoyalangan tarmoqni qurish imkoniyatiga ega himoya vositasi bu?   
+Virtual Private Network.   
199.Qaysi himoya vositasida mavjud paket shifrlangan holda yangi hosil qilingan mantiqiy paket ichiga kiritiladi?   
+Virtual Private Network.   
200.Qaysi himoya vositasi tarmoqda uzatilayotgan axborotni butunligi, maxfiyligi va tomonlar autentifikatsiyasini ta'minlaydi?   
+Virtual Private Network.   
201.Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi.   
+Tarmoqlararo ekran.