

Xato

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

Paranoid siyosat

Zaxiralashning qanday turlari mavjud?

Ichki, tashqi

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

Dastlabki virus nechanchi yilda yaratilgan?

1988

System-Specific Security Policies, 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 ... jumlaning 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, yaxlitlikni 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-:funktsiyaning natijasi ...

J: fiksirlangan uzunlikdagi xabar

Ethernet kontsentritori qanday vazifani bajaradi

J: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi

Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?

J: flashka, 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

Shifrtexstni 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 shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
sifatlariga ega bo'lishi kerak?

J: ishonchli, qimmatli va to'liq

Shifrlash –

J: akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifratnıga almashtiriladi

Qo'yish, o'rin almashtirish, gımmalash kriptografiyaning qaysi turiga bog'liq?

J: simmetrik kriptosistemalar

Foydalanishni boshqarish –bu...

J: Subyektnı 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 shifratnıga qo'shilgan qo'shimcha

Hab bu...

J: ko'plab tarmoqlarnı 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: Axborotlarnı o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish

Uning egasi haqiqiylikini 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 shifrnı 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 $k_1 \neq k_2$ bo'lib, k_1 ochiq kalit, k_2 yopiq kalit deb yuritiladi, k_1 bilan axborot shifrlanadi, k_2 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

Kriptografiya matn –

J: alifbo elementlarining tartiblangan to'plami

Autentifikatsiya jarayoni qanday jarayon?

J: obyekt yoki subhektning 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 shifmatnga 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

Kriptografiya 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 kriptotizimning 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 haqiqiylikni 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. Shifrtexstni 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 qobiliyatini aniqlashdir.
12. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?
J: Yulduz
13. RSA algoritmi qaysi yilda ishlab chiqilgan?
J: 1977 yil
14. Elektron xujjatlarni yo'q qilish usullari qaysilar?
J:Shredirlash, magnitsizlantirish, yanchish
15. Kriptografiya 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
2. Rezident virus...
tezkor xotirada saqlanadi
3. 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
4. O'chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.
Recuva, R.saver
5. Zaiflik – bu...
tizimda mavjud bo'lgan xavfsizlik muammoasi bo'lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.
6. Axborot xavfsizligi timsollarini ko'rsating.
Alisa, Bob, Eva
7. Kiberetika tushunchasi:
Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

8. "Axborot olish va kafolatlar va erkinligi to'g'risda"gi Qonuni qachon kuchga kirgan?
1997 yil 24 aprel
9. DIR viruslari nimani zararlaydi?
FAT tarkibini zararlaydi
10. 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
11. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi deb ataladi?
"Issiq zaxiralash"
12. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...
Tamoqlararo ekranlarning o'rnatilishi
13. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?
Axborot xavfsizligi buzulgan taqdirda ko'rilishi mumkin bo'lgan zarar miqdori bilan
14. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-...
Kiberjinoyat deb ataladi
15. Antiviruslarni, qo'llanish usuliga ko'ra... turlari mavjud?
detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar
16. Qaysi siyosatga ko'ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?
Ruxsat berishga asoslangan siyosat
17. DIR viruslari nimani zararlaydi?
FAT tarkibini zararlaydi
18. Makroviruslar nimalarni zararlaydi?
Ma'lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan "makros"lar yoki "skriptlar"ni zararlaydi.
19. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.
HandyBakcup
20. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa deb ataladi.
"Sovuq saxiralash"
21. "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
22. 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
23. 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 inshonchiligi, 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, yaxlitlikni 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 elementlari 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 ... jumlaning davom ettirish	shifrlash va shifrnı ochish uchun bitta va aynan shu kalitdan foydalaniladi
52.	Kriptobardoshlilik deb ...	kalitlarnı bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
53.	Elektron raqamli imzo deb –	xabar muallifi va tarkibini aniqlash maqsadida shifratga 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 –	kalitlarnı bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
57.	Shifrlash –	akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifratga 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 kriptotizimning 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?	$E_k1(T)=T$, $D_{k2}(T1)=T$
64.	Berilgan ta'riflardan qaysi biri assimmetrik tizimlarga xos?	Assimmetrik kriptotizimlarda $k1 \neq k2$ 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 elementlariga 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 assimmetrik
73.	Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?	Korporativ va umumfoydalanuvchi
74.	Elektromagnit nurlanish va ta'sirlanishlardan himoyalaniish 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 haqiqiylikini 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 sifatlariga 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 saqllovchi va tashuvchi vositalar qaysilar?	fleshka, CD va DVD disklar
87.	Imzo bu nima ?	hujjatning haqiqiylikini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati.
88.	Muhr bu nima?	hujjatning haqi-qiylikini 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 soʻzlarda kelish chastotasini yashirmaydi
92.	Axborot xavfsizligi va xavfsizlik sanʼati haqidagi fan deyiladi?	Kriptografiya
93.	Tekstni boshqa tekst ichida maʼnosini yashirib keltirish bu -	steganografiya
94.	Shifrtexstni ochiq tekstga akslantirish jarayoni nima deb ataladi?	Deshifrlash
95. – hisoblashga asoslangan bilim sohasi boʻlib, buzgʻunchilar mavjud boʻlgan jaroitda amallarni kafolatlash uchun oʻzida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.	Kiberxavfsizlik
96.	Risk	Potensial foyda yoki zarar
97.	Kiberxavfsizlik nechta bilim soxasini oʻz ichiga oladi.	8
98.	“Maʼlumotlar xavfsizligi” bilim sohasi.....	maʼlumotlarni saqlashda, qayta ishlashda va uzatishda himoyani taʼminlashni maqsad qiladi.
99.	“Dasturiy taʼminotlar xavfsizligi” bilim sohasi.....	foydalanilayotgan tizim yoki axborot xavfsizligini taʼminlovchi dasturiy taʼminotlarni ishlab chiqish va foydalanish jarayoniga eʼtibor qaratadi.
100.	“Tashkil etuvchilar xavfsizligi”	katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat koʻrsatishga eʼtibor qaratadi.
101.	“Aloqa xavfsizligi” bilim sohasi.....	tashkil etuvchilar oʻrtasidagi aloqani himoyalashga etibor qaratib, oʻzida fizik va mantiqiy ulanishni birlashtiradi.
102.	“Tizim xavfsizligi” bilim sohasi.....	tashkil etuvchilar, ulanishlar va dasturiy taʼminotdan iborat boʻlgan tizim xavfsizligining aspektlariga eʼtibor qaratadi.
103.	“Inson xavfsizligi” bilim sohasi....	kiberxavfsizlik bilan bogʻliq inson hatti harakatlarini oʻrganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy maʼlumotlarni va shaxsiy hayotni himoya qilishga eʼtibor qaratadi.
104.	“Tashkilot xavfsizligi” bilim sohasi	tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqiyatli bajarishini
105.	“Jamoat xavfsizligi” bilim sohasi	u yoki bu darajada jamiyatda taʼsir koʻrsatuvchi kiberxavfsizlik omillariga eʼtibor qaratadi.
106.	Tahdid nima? tizim yoki	Tashkilotga zarar yetkazishi mumkin boʻlgan istalmagan hodisa.
107.	Kodlash nima?	Maʼlumotni osongina qaytarish uchun hammaga ochiq boʻlgan sxema yordamida maʼlumotlarni boshqa formatga oʻzgartirishdir
108.	Shifrlash nima?	Maʼlumot boshqa formatga oʻzgartiriladi, biroq uni faqat maxsus shaxslar qayta oʻzgartirishi mumkin boʻladi
109.	Bir martalik bloknotda Qanday kalitlardan foydalaniladi?	Ochiq kalitdan
110.	Ikkilik sanoq tizimida berilgan 10111 sonini oʻnlik sanoq tizimiga oʻtkazing.	23
111.	Agar RSA algotirmida n ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.	$M = C^d \bmod n;$
112.	Oʻnlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq	100001

	tizi miga o'tkazing. 65	
113.	Quyidagi modulli ifodani qiymatini toping. $(125 \cdot 45) \bmod 10$.	5
114.	Quyidagi modulli ifodani qiymatini toping $(148 + 14432) \bmod 256$.	244
115.	Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.	$C = M^e \bmod n$; -tog'ri javob
116.	Axborotni shifrn 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 xabarlarini haqiqiylikni aniqlash, tashuvchilarda axborotlarni shifrlangan ko'rinishda saqlash (masalan, hujjatlarni, ma'lumotlar bazasini)
120.	Shifr nima?	Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritim
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'lumotlarni bitlar yoki belgilar bo'yicha shifrlaydi
123.	Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating.	uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmashligi uchun algoritim yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritimni maxfiyligiga emas, balki kalitni maxfiyligiga bog'liq bo'lishi lozim,
124.	Kriptotizim quyidagi komponentlardan iborat:	ochiq matnlar fazosi M, Kalitlar fazosi K, Shifratnlar fazosi C, Ek : $M \rightarrow C$ (shifrlash uchun) va Dk: $C \rightarrow M$ (deshifrlash uchun) funktsiyalar
125.	Serpent, Square, Twofish, RC6 , AES algoritmlari qaysi turiga mansub?	simmetrik blokli algoritmlar
126.	DES algoritimga muqobil bo'lgan algoritimni ko'rsating.	Uch karrali DES, IDEA, Rijndael
127.	DES algoritmining asosiy muammosi nimada?	kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshlilik uchun yetarli emas
128.	Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?	shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun
129.	$12+22 \bmod 32$?	2
130.	$2+5 \bmod 32$?	7
131.	Kriptografik elektron raqamli imzolarda qaysi kalitlar ma'lumotni yaxlitligini ta'minlashda ishlatiladi.	ochiq kalitlar
132.	$12+11 \bmod 16$?	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	Xesh funktsiyalar

	oshiriladi	
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 qoidalarini 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 modelining amaliy 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 tembr.	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 qobiliyatini aniqlashdir.
169.	Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi,	Sub'ekt
170.	Foydalanishni 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 qoidalarini 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 muvaffaqiyatli 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, foydalanuvchilarga 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 haqiqiyiligini tekshirish qaysi kalit yordamida amalga oshiriladi?	Imzo muallifining ochiq <i>kaliti yordamida</i>
211.	Tarmoq modeli-bu...	Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat'iy nazar muvaffaqiyatli 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	Transport
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'xtat 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'xtat 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'lumotlarini kutilmaganda oshkor bo'lishi ushbu xodimlarga bevosita ta'sir qiladi
247.	Quyidagi ta'riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi	Tarmoq qurilmalari, switch 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 maqsadda 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 xususiyatiga berilgan ta'rifni nelingilash	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 topish
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 zaxiralash 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 tarmoqqa 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	«Chualchag» 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, vaksinalar, 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, yaxlitlikni 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'rinishdagi 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 prinsipiga 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.	$256 \bmod 25 = ?$	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 duvidadi	Xavfsizlik siyosati
316.	RSA shifrlash algoritmidan foydalaniladigan sonlarning spektri o'lchami qanday?	p va q –sonlarning ko'paytmasini ifodalovchi sonning spektriga 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 funksiyasida $\phi(1)$ 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 $(148 + 14432) \bmod 256$.	244
327.	Quyidagi sonlarning eng katta umumiy bo'luvchilarini toping. 88 i 220	44
328.	Quyidagi ifodani qiymatini toping. $-17 \bmod 11$	5
329.	2 soniga 10 modul bo'yicha teskari sonni toping.	\emptyset
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 sathi 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 -	RH 45-185:2011

	Xujjat raqamini toping	
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.	Smartkarta 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 qobiliyatini 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	Discretionary access control DAC

	operatsion tizimlarda qo'llaniladi?	
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'miga 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 maslahatlar
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 arxitekturasini nechta tashkil etuvchidan iborat?	5
392.	WiMAX tarmoq arxitekturasini qaysi tashkil etuvchidan	Base station, Subscriber station, Mobile station, Relay

	iborat?	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.	Shredder
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, Trojan 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 printsipligiga 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 siyosatining 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 arxitekturasini
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 inshonchiligi, 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, yaxlitlikni 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 shifrnin 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 ... jumlaning davom ettiring	*shifrlash va shifrnı ochish uchun bitta va aynan shu kalitdan foydalaniladi
465.	Kriptobardoshlilik deb ...	*kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
466.	Elektron raqamli imzo deb –	*xabar muallifi va tarkibini aniqlash maqsadida shifratma 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 shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
470.	Shifrlash –	*akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifratma almashiriladi
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 shifrlama matnlar tayyorlash harakatlaridan iborat jarayon
473.	Blokli shifrlash-	*shifrlanadigan matn blokiga qo'llaniladigan asosiy akslantirish
474.	Simmetrik kriptotizimning uzluksiz tizimida ...	*ochiq matnning har bir harfi va simvoli alohida shifrlanadi
475.	Kripto tizimga qo'yiladigan umumiy talablardan biri	*shifrlama matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak
476.	Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos?	*Asimmetrik kriptotizimlarda $k_1 \neq k_2$ bo'lib, k_1 ochiq kalit, k_2 yopiq kalit deb yuritiladi, k_1 bilan axborot shifrlanadi, k_2 bilan esa deshifrlanadi
477.	Yetarlicha kriptotizimning unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang	*Vijener matritsasi, Sesar usuli
478.	Akslantirish tushunchasi deb nimaga aytiladi?	*1-to'plamli elementlariga 2-to'plamli elementlariga 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 asimmetrik

485.	Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?	*Korporativ va umumfoydalanuvchi
486.	Elektromagnit nurlanish va ta'sirlanishlardan himoyalaniş 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 haqiqiylikini 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 haqiqiylikini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati.
500.	Muhr bu nima?	*hujjatning haqiqiylikini 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.	Shifrttekstni 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 shifrnı 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?	Elektron raqamli imzo; kalitlarni boshqarish
515.	Kriptografik usullardan foydalanishning asosiy yo'nalishlari nimalardan iborat?	uzatiliyotgan xabarlarini haqiqiylikini aniqlash
516.	Shifr nima?	* Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritmi
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'lumotlarni bitlar yoki belgilar bo'yicha shifrlaydi
519.	Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating.	*uzatiliyotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmashligi uchun algoritmi yetarli darajada bardoshli bo'lishi lozim, uzatiliyotgan xabarni xavfsizligi algoritmi maxfiyligiga emas, balki kalitni maxfiyligiga bog'liq bo'lishi lozim,
520.	Kriptotizim qaysi komponentlardan iborat?	*ochiq matnlar fazosi M, Kalitlar fazosi K, Shifmatnlar fazosi C, Ek : $M \rightarrow C$ (shifrlash uchun) va Dk: $C \rightarrow M$ (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 algoritmlar orqali amalga oshiriladi	*Xesh funktsiyalar
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	*Taqqimlash satxi
538.	OSI modelining yettinchi satxi qanday nomlanadi	*Amaliy satx
539.	OSI modelining qaysi satxlari tarmoqqa bog'liq satxlar	*fizik, kanal va tarmoq satxlari

	hisoblanadi	
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 funksiyalarni bajaradi	*Elektr signallarini uzatish va qabul qilish
546.	OSI modelining amaliy satxi qanday funksiyalarni 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...	Subyektning Subyektga ishlash qobiliyatini aniqlashdir.
557.	Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?	Obyekt
558.	Foydalanishni boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ?	*Obyekt
559.	Foydalanishni 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	*Yozish

	darajasida bo'lsa, u holda qanday amalga ruxsat beriladi.	
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'rtasida 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, foydalanuvchilarga	Razvedka hujumlari

	va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi;	
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 - $\varphi(n)$ bilan o'zaro tub
598.	RSA elektron raqamli imzo algoritmidagi yopiq kalit d qanday hisoblanadi? Bu yerda p va q tub sonlar, $n=pq$, $\varphi(n)$ - Eyler funksiyasi, e-ochiq kalit	* $d = e^{-1} \bmod \varphi(n)$
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 <i>kaliti yordamida</i>
601.	Tarmoq modeli-bu...	*Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat'iy nazar muvaffaqiyatli 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 protokolinig necha xil versiyasi mavjud?	1
633.	Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang	*Ichki, tashqi
634.	Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlariga olib keladi	*Biznes jarayonlarni to'xtat qolishiga olib keladi
635.	Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo'qolishi qanday oqibatlariga olib keladi	Biznesda ixtiyoriy hujum biznes jarayonlarni to'xtat qolishiga olib keladi
636.	Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo'qolishi qanday oqibatlariga olib keladi	Biznesda ixtiyoriy hujum biznes jarayonlarni to'xtat qolishiga olib keladi
637.	Tarmoq xavfsizligining buzilishi natijasida axborotning o'g'irlanishi qanday oqibatlariga olib keladi	Biznesda ixtiyoriy hujum biznes jarayonlarni to'xtat qolishiga olib keladi
638.	Quyidagi ta'riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi	*Tarmoq qurilmalari, switch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo'lmasligi
639.	Quyidagi ta'riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi	Tarmoq qurilmalari, switch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo'lmasligi
640.	Quyidagi ta'riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi.	Tarmoq qurilmalari, switch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo'lmasligi
641.	Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqsadda 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 axborotni 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	paket filterlari tarmoq satxida ishlaydi; ekspert paketi

	bo'lindi?	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 sahida ishlaydi; 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 funkcionallikni 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 funkcionallikni 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 funkcionallikni 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 funkcionallikni 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 funkcionallikni 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 <i>ishonchlilik</i> 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	*Taqdirlash 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 modelining amaliy 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 topish
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.	Differensial 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 anizilini 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, yaxlitlikni 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 asoslanganbu 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 asoslanganbu 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'rnuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi
743.	Rootkitlar-	bir qarashda yaxshi va foydali kabi ko'rnuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi
744.	Backdoorlar -	bir qarashda yaxshi va foydali kabi ko'rnuvchi dasturiy vositasifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi
745.	Troyan otlari-	*bir qarashda yaxshi va foydali kabi ko'rnuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi
746.	Ransomware-	bir qarashda yaxshi va foydali kabi ko'rnuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi
747.	Resurslardan foydalanish usuliga ko'ra viruslar qanday	*Virus parazit, Virus cherv

	turlarga bo'linadi	
748.	Zararlagan obyektlar turiga ko'ra	Virus parazit, Virus cherv
749.	Faollashish prinsipiga 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 zararlasi, 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 zararlasi, 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 zararlasi, 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 zararlasi, 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.	$256 \bmod 25 = ?$	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 duydadi	Standart
763.	RSA shifrlash algoritmidan 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 algoritmilarining 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	$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$
770.	Eyler funsiyasida $\phi(1)$ 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'ring.
780. +: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik
781. -: Axborot va Iqtisodiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xavfsizligi, Dasturiy ta'minot xavfsizligi
782. -: Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xavfsizligi, Ekologik xavfsizlik
783. -: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Dasturiy ta'minot xavfsizligi, Ekologik xavfsizlik
784. I:
785. S: Axborot xavfsizligining asosiy maqsadlaridan biri- bu...
786. +: Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish
787. -:Ob'yektga bevosita ta'sir qilish
788. -: Axborotlarni shifrlash, saqlash, yetkazib berish
789. -: Tarmoqdagi foydalanuvchilarni xavfsizligini ta'minlab berish
790. I:
791. S: Konfidentsiallikga to'g'ri ta'rif keltiring.
792. +: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
793. -:axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati;
794. -:axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati;
795. -:axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati;
796. I:
797. S: Yaxlitlikni buzilishi bu - ...
798. +: Soxtalashtirish va o'zgartirish
799. -: Ishonchsizlik va soxtalashtirish
800. -: Soxtalashtirish
801. -: Butunmaslik va yaxlitlanmaganlik
802. I:
803. 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
805. -: 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

806. -: 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
807. -: 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
808. I:
809. S: Kompyuter virusi nima?
810. +: maxsus yozilgan va zararli dastur
811. -: .exe fayl
812. -: boshqariluvchi dastur
813. -: Kengaytmaga ega bo'lgan fayl
814. I:
815. S: Kriptografiyaning asosiy maqsadi...
816. +: maxfiylik, yaxlitlikni ta'minlash
817. -: ishonchlilik, butunlilikni ta'minlash
818. -: autentifikatsiya, identifikatsiya
819. -: ishonchlilik, butunlilikni ta'minlash, autentifikatsiya, identifikatsiya
820. I:
821. S: SMTP - Simple Mail Transfer protokol nima?
822. +: elektron pochta protokoli
823. -: transport protokoli
824. -: internet protokoli
825. -: Internetda ommaviy tus olgan dastur
826. I:
827. S: SKIP protokoli...
828. +: Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi
829. -: Protokollar boshqaruvi
830. -: E-mail protokoli
831. -: Lokal tarmoq protokollari uchun kriptokalitlarning oddiy boshqaruvi
832. I:
833. S: Kompyuter tarmog'ining asosiy komponentlariga nisbatan xavf-xatarlar...
834. +: uzilish, tutib qolish, o'zgartirish, soxtalashtirish
835. -: o'zgartirish, soxtalashtirish
836. -: tutib qolish, o'zgarish, uzilish
837. -: soxtalashtirish, uzilish, o'zgartirish
838. I:
839. S: ...ma'lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.
840. +: konfidentsiallik
841. -: identifikatsiya
842. -: autentifikatsiya
843. -: maxfiylik
844. I:
845. S: Foydalanish huquqini cheklovchi matritsa modeli bu...
846. +: Bella La-Padulla modeli
847. -: Denning modeli
848. -: Landver modeli
849. -: Huquqlarni cheklovchi model
850. I:
851. 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
859. -: Tizim meyoriy va g'ayritabiiy hollarda rejalashtirilgandek o'zini tutishligi holati
860. -: Istalgan vaqtda dastur majmuasining mumkinligini kafolati
861. -:Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi
862. I:
863. S:Identifikatsiya bu- ...
864. +: Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni
865. -:Ishonchliligini tarqalishi mumkin emasligi kafolati
866. -:Axborot boshlang'ich ko'rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o'zgarishlar
867. -:Axborotni butunligini saqlab qolgan holda uni elementlarini o'zgartirishga yo'l qo'ymaslik
868. I:
869. S:O'rin almashtirish shifri bu - ...
870. +: Murakkab bo'lmagan kriptografik akslantirish
871. -:Kalit asosida generatsiya qilish
872. -:Ketma-ket ochiq matnni ustiga qo'yish
873. -:Belgilangan biror uzunliklarga bo'lib chiqib shifrlash
874. I:
875. S:Simmetrik kalitli shifrlash tizimi necha turga bo'linadi.
876. +: 2 turga
877. -:3 turga
878. -:4 turga
879. -: 5 turga
880. I:
881. S: Kalitlar boshqaruvi 3 ta elementga ega bo'lgan axborot almashinish jarayonidir bular ...
882. +: hosil qilish, yig'ish, taqsimlash
883. -:ishonchliligi, maxfiyligi, aniqligi
884. -:xavfsizlik, tez ishlashi, to'g'ri taqsimlanishi
885. -:abonentlar soni, xavfsizligi, maxfiyligi
886. I:
887. S: Kriptologiya -
888. +: axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi
889. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
890. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o'rganadi
891. -:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
892. I:
893. S: Kriptografiyada alifbo –
894. +: axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam
895. -:matnni shifrlash va shifrni ochish uchun kerakli axborot
896. -:xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo'shilgan qo'shimcha
897. -:kalit axborotni shifrllovchi kalitlar
898. I:
899. S: Simmetrik kriptotizimlarda ... jumlani davom ettiring
900. +: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi
901. -:bir-biriga matematik usullar bilan bog'langan ochiq va yopiq kalitlardan foydalaniladi
902. -:axborot ochiq kalit yordamida shifrlanadi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi
903. -:kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi

904. I:
 905. S: Kriptobardoshlilik deb ...
 906. +: kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
 907. -:axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi
 908. -:kalitni bilmasdan shifrlangan matnnı ochish imkoniyatlarini o'rganadi
 909. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
 910. I:
 911. S: Elektron raqamli imzo deb –
 912. +: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo'shilgan qo'shimcha
 913. -:matnnı shifrlash va shifrnı ochish uchun kerakli axborot
 914. -:axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam
 915. -:kalit axborotni shifrovchi kalitlar
 916. I:
 917. S: Kriptografiya –
 918. +: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
 919. -:axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi
 920. -:kalitni bilmasdan shifrlangan matnnı ochish imkoniyatlarini o'rganadi
 921. -:kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
 922. I:
 923. S: Kriptografiyada matn –
 924. +: alifbo elementlarining tartiblangan to'plami
 925. -:matnnı shifrlash va shifrnı ochish uchun kerakli axborot
 926. -:axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam
 927. -:kalit axborotni shifrovchi kalitlar
 928. I:
 929. S: Kriptoanaliz –
 930. +: kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
 931. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
 932. -:axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi
 933. -:kalitni bilmasdan shifrlangan matnnı ochish imkoniyatlarini o'rganadi
 934. I:
 935. S: Shifrlash –
 936. +: akslantirish jarayoni ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi
 937. -:kalit asosida shifrmatn ochiq matnga akslantiriladi
 938. -:shifrlashga teskari jarayon
 939. -:Almashtirish jarayoni bo'lib: ochiq matn deb nomlanadigan matn o'girilgan holatga almashtiriladi
 940. I:
 941. S: Faol hujum turi deb...
 942. +: Maxfiy uzatish jarayonini uzib qo'yish, modifikatsiyalash, qalbaki shifr ma'lumotlar tayyorlash harakatlaridan iborat jarayon
 943. -:Maxfiy ma'lumotni aloqa tarmog'ida uzatilayotganda eshitish, tahrir qilish, yozib olish harakatlaridan iborat uzatilalayotgan ma'lumotni qabul qiluvchiga o'zgartirishsiz yetkazish jarayoni
 944. -:Ma'lumotga o'zgartirish kiritmay uni kuzatish jarayoni
 945. -:Sust hujumdan farq qilmaydigan jarayon
 946. I:
 947. S: Blokli shifrlash-
 948. +: shifrlanadigan matn blokiga qo'llaniladigan asosiy akslantirish
 949. -:murakkab bo'lmagan kriptografik akslantirish
 950. -:axborot simvollarini boshqa alfavit simvolları bilan almashtirish
 951. -:ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi
 952. I:
 953. S: Simmetrik kriptotizimning uzluksiz tizimida ...

954. +: ochiq matnning har bir harfi va simvoli alohida shifrlanadi
955. -:belgilangan biror uzunliklarga teng bo'linib chiqib shifrlanadi
956. -:murakkab bo'lmagan kriptografik akslantirish orqali shifrlanadi
957. -:ketma-ket ochiq matnlarni o'rniga qo'yish orqali shifrlanadi
958. I:
959. S: Kriptotizimga qo'yiladigan umumiy talablardan biri
960. +: shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak
961. -:shifrlash algoritmining tarkibiy elementlarini o'zgartirish imkoniyati bo'lishi lozim
962. -:ketma-ket qo'llaniladigan kalitlar o'rtasida oddiy va oson bog'liqlik bo'lishi kerak
963. -:maxfiylik o'ta yuqori darajada bo'lmoqligi lozim
964. I:
965. S: Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos?
966. +: Asimmetrik kriptotizimlarda $k_1 \neq k_2$ bo'lib, k_1 ochiq kalit, k_2 yopiq kalit deb yuritiladi, k_1 bilan axborot shifrlanadi, k_2 bilan esa deshifrlanadi
967. -:Asimmetrik tizimlarda $k_1 = k_2$ bo'ladi, yahni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi
968. -:Asimmetrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma'lum bo'ladi, ochiq kalitni esa faqat qabul qiluvchi biladi
969. -:Asimmetrik kriptotizimlarda $k_1 \neq k_2$ bo'lib, kalitlar hammaga oshkor etiladi
970. I:
971. S: Yetarlicha kriptoturg'unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang
972. +: Vijener matritsasi, Sezar usuli
973. -:monoalfavitli almashtirish
974. -:polialfavitli almashtirish
975. -:o'rin almashtirish
976. I:
977. S: Akslantirish tushunchasi deb nimaga aytiladi?
978. +: 1-to'plamli elementlariga 2-to'plam elementlariga mos bo'lishiga
979. -:1-to'plamli elementlariga 2-to'plam elementlarini qarama-qarshiligiga
980. -:har bir elementni o'ziga ko'payimasiga
981. -:agar birinchi va ikkinchi to'plam bir qiymatga ega bulmasa
982. I:
983. S: Simmetrik guruh deb nimaga aytiladi?
984. +: O'rin almashtirish va joylashtirish
985. -:O'rin almashtirish va solishtirish
986. -:Joylashtirish va solishtirish
987. -:O'rin almashtirish va transportizatsiyalash
988. I:
989. S: Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq?
990. +: simmetrik kriptosistemalar
991. -:assimetrik kriptosistemalar
992. -:ochiq kalitli kriptosistemalar
993. -:autentifikatsiyalash
994. I:
995. 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 subhekttni 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 subhekttni 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 subhekttni 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 shifrnı 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 kriptografik 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'lumotlarni 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'lmashligi uchun algoritm yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiylikiga emas, balki kalitni maxfiylikiga bog'liq bo'lishi lozim,
 1119. -:uzatilayotgan xabarni xavfsizligi kalitni maxfiylikiga emas, balki algoritmni maxfiylikiga 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 imzolarida 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. -:Taqqdimlash 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. -:Taqqdimlash 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 amalg'a 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. -:Vakolatlarni 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. -:biometrik alomatlarining ishga layoqatli shaxsdan ajratib bo'lmazligi
1312. -:biometrik alomatlarini soxtalashtirishning qiyinligi
1313. -:biometrik alomatlarini 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'rtasida 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 barcha chiquvchi 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:
1399. S: Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi;
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, foydalanuvchilarga 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 - $\varphi(n)$ 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, $n=pq$, $\varphi(n)$ - Eyler funksiyasi,e-ochiq kalit
 1430. +: $d = e^{-1} \bmod \varphi(n)$
 1431. -: $d = e^{-1} \bmod q$
 1432. -: $d = e^{-1} \bmod q$
 1433. -: $d = e^{-1} \bmod p$
 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

 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 muvaffaqiyatli 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. -:Transport
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. -:Transport
1469. -:Ilova, taqdimot, seans.
1470. I:
1471. S: TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi
1472. +: Transport
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. -:Transport
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 maqsadda 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 funksiyalarni 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. -:Taqdirlash satxi
1607. I:
1608. S: OSI modelining oltinchi satxi qanday nomlanadi
1609. +: Taqdirlash 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. -:Taqdirlash 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 modelining amaliy 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 signallarini uzatish va qabul qilish
1643. I:
1644. S: Yevklid algoritmi qanday natijani beradi?
1645. +: Sonning eng katta umumiy bo'luvchisini topish
1646. -:Soning turli bo'luvchilarini topish
1647. -:Soning eng kichik umumiy karralisini topish
1648. -:Soning 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. +: «Chualchang» va replikatorli virus
1712. -:Kvazivirus va troyan virus
1713. -:Trojan 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: Trojan 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, yaxlitlikni ta'minlash
1772. -:ishonchlilik, butunlikni ta'minlash
1773. -:autentifikatsiya, identifikatsiya
1774. -:ishonchlilik, butunlikni 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 qoldikli bo'lish qonunini ifodalaydi
1801. +: $a = bq + r, 0 \leq r \leq b$,
1802. -: $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$
1803. -: $M=r1^k2$;

1804. -: $M = \sqrt{k_1 + k_2}$
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. $(148 + 14432) \bmod 256$.
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. $-16 \bmod 11$
1838. +: 6
1839. -: 5
1840. -: 7
1841. -: 11
1842. I:
1843. S: 2 soniga 10 modul bo'yicha teskari sonni toping.
1844. +: \emptyset
1845. -: 3
1846. -: 10
1847. -: 25
1848. I:
1849. S: 2 soniga 10 modul bo'yicha teskari sonni toping.
1850. +: \emptyset
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. -: 2^{64} modul bo'yicha qo'shish
1894. -: 2^{32} modul bo'yicha qo'shish
1895. -: 2^{48} modul bo'yicha qo'shish
1896. I:
1897. S: $4+31 \bmod 32$?
1898. +:3
1899. -:4
1900. -:31
1901. -:32
1902. I:
1903. S: $21+20 \bmod 32$?
1904. +:9
1905. -:12
1906. -:16
1907. -:41
1908. I:

1909. S: $12+22 \bmod 32$?
1910. +:2
1911. -:12
1912. -:22
1913. -:32
1914. I:
1915. S: AES algoritmi bloki uzunligi ... bitdan kam bo'lmash 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: $2+5 \bmod 32$?
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. $-17 \bmod 11$
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 hisoblanadi.
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 muhimligi 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. -:Tabiiy 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 konfedsialligi
2104. -: Foydalanuvchanligi
2105. -: Ixchamligi }
2106. I:
2107. S: Axborotning buzilishi yoki yo'qotilishi xavfiga olib keluvchi himoyalalanuvchi 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 alomatlarining 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 konfedsialligi
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 himoyalashni 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. -:Identifikatsiya
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 ishlaymay turganda yoki foydalanuvchilar ma'lumot bilan ishlaymay 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. +:HandyBackup
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, kompyuterlar 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: litsenziyalik 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 qadrlilik 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 autentifikatsiyalashdan 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 qoidalarini 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 qoidalarini 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 soʻzini 3 kalit bilan shifrlagandan soʻng qaysi soʻz hosil boʻladi.
A=0, B=1....Z=25.
2439. +:GDGD
2440. -: NANA
2441. -: GPGP
2442. -: FDFD
2443. I:
2444. S: Lotin alifbosida NON soʻzini 3 kalit bilan shifrlagandan soʻng qaysi soʻz hosil boʻladi.
A=0, B=1....Z=25.
2445. -:GDGD
2446. -: NANA
2447. +: QRQ
2448. -: FDFD
2449. I:
2450. S: Fizik toʻsiqlarni oʻrnatish , Xavfsizlik qoʻriqchilarini ishga olish, Fizik qulflar qoʻyishni amalga oshirish qanday nazorat turiga kiradi?
2451. +:Fizik nazorat
2452. -: Texnik nazorat
2453. -: Maʼmuriy nazorat
2454. -: Tashkiliy nazorat
2455. I:
2456. S: Ruksatlarni nazoratlash, “Qopqon”, Yongʻinga 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. -: Maʼmuriy nazorat
2460. -: Tashkiliy nazorat
2461. I:
2462. S: Qoida va muolajalarni yaratish, Joylashuv arxitekturasini loyihalash, Xavfsizlik belgilari va ogohlantirish signallari, Ishchi joy xavfsizligini taʼminlash, Shaxs xavfsizligini taʼminlash amalga oshirish qanday nazorat turiga kiradi?
2463. -: Fizik nazorat
2464. -: Texnik nazorat
2465. +: Maʼmuriy 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 xavflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak.
 2513. -: Kamida 6 belgi: katta va kichik xavflar, 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 qobiliyatini 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 kriptografik 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, yaxlitlikni 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 kriptografik algoritim

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.

HandyBackup

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 "makros"lar yoki "skriptlar"ni zararlaydi.

3. Ehtiyotkorlik siyosati (Prudent Policy) – bu

Barcha xizmatlar 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. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?

Paranoid siyosati (Paranoid 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 himoyalaniishi 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 maqsadda amalga oshiriladigan tarmoq hujumi qaysi?

Razvedka hujumlari

1. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?

Paranoid siyosati (Paranoid 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 buzilgan 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. Dastlabki virus nechanchi yilda yaratilgan?

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 maqsadda 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 vositalari – bu ...

Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob'ektni himoyalashdir

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 xavfsizligini 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, yaxlitlikni ta'minlash

4. Uning egasi haqiqiylikni 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, yaxlitlikni 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 $k_1 \neq k_2$ bo'lib, k_1 ochiq kalit, k_2 yopiq kalit deb yuritiladi, k_1 bilan axborot shifrlanadi, k_2 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.

HandyBackup

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 himoyalaniishi lozim bo'lgan narsalar

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

...

Kracker

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. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?

Paranoid siyosati (Paranoid 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 himoyalaniishi 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 Administrator xavfsiz va zarur xizmatlarga individual 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 $k_1 \neq k_2$ bo'lib, k_1 ochiq kalit, k_2 yopiq kalit deb yuritiladi, k_1 bilan axborot shifrlanadi, k_2 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 qobiliyatini aniqlashdir.

3. Uning egasi haqiqiyiligini 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. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?

Paranoid siyosati (Paranoid 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 -

Kraker

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. Dastlabki virus nechanchi yilda yaratilgan?

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 kriptografik 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. Dastlabki virus nechanchi yilda yaratilgan?

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 vositalari – bu ...

Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob'ektni himoyalashdir

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 -

...

Kraker

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. Dastlabki virus nechanchi yilda yaratilgan?

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

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 konfidentsialligi, 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 aytiladi? =====

#kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi=====

axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi=====

kalitni bilmasdan shifrlangan matnnı 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 $k_1 \neq k_2$ bo'lib, k_1 ochiq kalit, k_2 yopiq kalit deb yuritiladi, k_1 bilan axborot shifrlanadi, k_2 bilan esa deshifrlanadi====

Assimetrikrik tizimlarda $k_1 = k_2$ 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 $k_1 \neq k_2$ 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 haqiqiylikini aniqlash jarayonida matnhiruv axboroti sifatida ishlatiladigan belgilar

ketma-ketligi (maxfiy soʻz) – nima? =====

#parol=====

login=====

identifikatsiya=====

maxfiy maydon

++++

Roʻyxatdan oʻtish-bu...=====

#foydalanuvchilarni roʻyxatga olish va ularga dasturlar va maʼlumotlarni ishlatishga huquq berish jarayoni=====

axborot tizimlari obʼyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom boʻyicha solishtirib uni aniqlash jarayoni=====

obyekt yoki subhektning 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 boʻlishi kerak? =====

#ishonchli, qimmatli va toʻliq=====

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

++++

Shifratntni 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 =====

Shifratntni 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 shifrnı 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 konfidentsialligi=====

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 himoyalaniishi 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

++++

“Hamma narsa ta'qiqlanadi.” Bu qaysi xavfsizlik siyosatiga xos?=====

Ruxsat berishga asoslangan siyosat (Permissive Policy)=====

#Paranoid siyosati (Paranoid Policy)=====

Ehtiyotkorlik siyosati (Prudent Policy)=====

Nomuntazam siyosat (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 Administrator xavfsiz va zarur xizmatlarga individual 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 xizmatlar/hujumlar/harakatlar bloklanadi=====

Hamma narsa ta’qiqlanadi=====

Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi=====

#Barcha xizmatlar 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 muvaffaqiyatli 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 xususiyati.=====

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

++++

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

#Ikki 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,megabayt,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 xarakteristikalariga 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 simvollarini bilan almashtirish=====

ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi

++++

Elektron pochtaga kirishda foydalanuvchi qanday autentifikatsiyalashdan o'tadi? =====

#Parol asosida=====

Smart karta asosida=====

Biometrik asosida=====

Ikki tomonlama

++++

Elektron raqamli imzo - bu ...=====

#xabar muallifi va tarkibini aniqlash maqsadida shifratga 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 ro'yxatga 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 imzolarida 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'lumotlarni 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 arxitekturasini 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 siyosatlarini ...=====

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, shifratga 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

++++

.... – oʻzida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi maʼlumoti va xavfsizlik algoritmlarini saqlaydi.=====

#Sim karta =====

Token =====

Smart karta =====

Elektron raqamli imzo

+++++

.... kompyuter tarmoqlari boʻyicha tarqalib, kompyuterlarning tarmoqdagi manzilini aniqlaydi va u yerda oʻzining nusxasini qoldiradi.=====

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

Kvazivirus va troyan virus=====

Troyan dasturi=====

Mantiqiy bomba

+++++

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

#tashkil etuvchilar oʻrtasidagi aloqani himoyalashga etibor qaratib, oʻzida fizik va mantiqiy ulanishni birlashtiradi.=====

katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat koʻrsatishga eʼtibor qaratadi.=====

foydalanilayotgan tizim yoki axborot xavfsizligini taʼminlovchi dasturiy taʼminotlarni ishlab chiqish va foydalanish jarayoniga eʼtibor qaratadi.=====

kiberxavfsizlik bilan bogʻliq inson hatti harakatlarini oʻrganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy maʼlumotlarni va shaxsiy hayotni himoya qilishga eʼtibor 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 muvaffaqiyatli 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'rinishdagi 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?=====

$M = C^d \bmod n$; =====

$C = M^d \bmod n$; =====

$C = M^{ed} \bmod n$; =====

$M = C^e \bmod n$;

++++

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=====

Global tarmoqdan uzib qo'yish=====

Aloqa kanallarida optik toladan foydalanish

++++

Akslantirish tushunchasi deb nimaga aytiladi? =====

#1-to'plamli elementlariga 2-to'plam elementaliga mos bo'lishiga=====

1-to'plamli elementlariga 2-to'plam elementalini qarama-qarshiligiga=====

har bir elementni o'ziga ko'payimasiga=====

agar birinchi va ikkinchi 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 va 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 maqsadida amalga oshiriladigan tarmoq hujumini belgilang. =====

#Razvedka hujumlari=====

Kirish hujumlari=====

DOS hujumi=====

Zararli hujumlar

++++

Attribute based access control ABAC usuli attributlari qaysilar? =====

#Foydalanuvchi attributlari=====

Asosiy va qo'shimcha atributlar =====

Tizim attributlari, server atributlari =====

Ichki va tashqi atributlar

++++

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

++++

Axborot tizimlari xavfsizligining auditi-bu...=====

#Axborot tizimlarining himoyalaniishining joriy holati, tizim haqida obyektiv ma'lumotlarni olish va baholash=====

Ma'lumotlarini tahlillash va chora ko'rishni tizim haqida subyektiv ma'lumotlarni olish va baholashni tahlil qiladi=====

Ma'lumotlarini tarqatish va boshqarish=====

Axborotni 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 obyektini qaysi xususiyatiga 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

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 shifrnı 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, yaxlitlikni 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:-funktsiyanı natijasi ...

J: fiksirlangan uzunlikdagi xabar

Ethernet kontsentratori qanday vazifani bajaradi

J: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi

Axborotlarni saqllovchi 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

Shifrttekstni 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 inshonchiligi, 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 shifratga almashtiriladi

Qo'yish, o'rin almashtirish, garmalash 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 qoidalarini 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 shifratnga 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 haqiqiylikni 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 shifrnı 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 $k_1 \neq k_2$ bo'lib, k_1 ochiq kalit, k_2 yopiq kalit deb yuritiladi, k_1 bilan axborot shifrlanadi, k_2 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 shifratnga 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 kriptotizimning 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

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, yaxlitlikni 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 elementlari 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 shifrnini ochish uchun kerakli axborot
20	Qo'yish, o'rin almashtirish, garmalash 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 ... jumlaning davom ettiring	shifrlash va shifrnini ochish uchun bitta va aynan shu kalitdan foydalaniladi
29	Kriptobardoshlilik deb ...	kalitlarni bilmasdan shifrnini ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
30	Elektron raqamli imzo deb –	xabar muallifi va tarkibini aniqlash maqsadida shifmatga 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 shifrnini 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?	$E_{k1}(T)=T$, $D_{k2}(T1)=T$
41	Berilgan ta'riflardan qaysi biri assimmetrik tizimlarga xos?	Assimmetrik kriptotizimlarda $k1 \neq k2$ 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 elementlariga mos bo'lishiga
44	Simmetrik guruh deb nimaga aytiladi?	O'rin almashtirish va joylashtirish
45	Qo'yish, o'rin almashtirish, garmalash kriptografiyaning qaysi turiga bog'liq?	simmetrik kriptosistemalar
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 assimmetrik
50	Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?	Korporativ va umumfoydalanuvchi

51	Elektromagnit nurlanish va ta`sirlanishlardan himoyalalanish 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 haqiqiylikini 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 haqiqiylikini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati.
65	Muhr bu nima?	hujjatning haqi-qiylikini 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	Shifrttekstni 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 sohasini 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 muvaffaqiyatli 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.	$M = C^d \bmod n$;
89	O‘nlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq tizi miga o‘tkazing. 65	100001
90	Quyidagi modulli ifodani qiymatini toping. $(125 \cdot 45) \bmod 10$.	5
91	Quyidagi modulli ifodani qiymatini toping $(148 + 14432) \bmod 256$.	244
92	Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.	$C = M^e \bmod n$; -tog‘ri javob
93	Axborotni shifrnı 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 xabarlarini 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 kriptografik algoritmlar
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 imkonini 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'lumotlarni bitlar yoki belgilar bo'yicha shifrlaydi
100	Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating.	uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmazligi uchun algoritmlar yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmlarni maxfiyligiga emas, balki kalitni maxfiyligiga bog'liq bo'lishi lozim,
101	Kriptotizim quyidagi komponentlardan iborat:	ochiq matnlar fazosi M, Kalitlar fazosi K, Shifmatnlar 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 algoritmgiga 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	$12+22 \bmod 32$?	2
107	$2+5 \bmod 32$?	7
108	Kriptografik elektron raqamli imzolarda qaysi kalitlar ma'lumotni yaxlitligini ta'minlashda ishlatiladi.	ochiq kalitlar
109	$12+11 \bmod 16$?	7
110	RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo'llab quvvatlaydi.	128 bitli, 192 bitli, 256 bitli
111	Xesh-funksiyani 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 modelining amaliy 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 tembr.	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 qobiliyatini aniqlashdir.
146	Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi,	Sub'ekt
147	Foydalanishni boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ?	Ob'ekt
148	Foydalanishni 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 muvaffaqiyatli 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 haqiqiyiligini 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 muvaffaqiyatli 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	Transport
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'lumotlarini kutilmaganda oshkor bo'lishi ushbu xodimlarga bevosita ta'sir qiladi
224	Quyidagi ta'riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi	Tarmoq qurilmalari, switch 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 maqsadda 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 tarmoqqa bog'lanish amalga 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, yaxlitlikni 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	Trojan otlari-	bir qarashda yaxshi va foydali kabi ko'rinishdagi dasturiy vosita sifatida ko'rsatib, yashiringan zararli kodlardan 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 prinsipiga 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	$256 \bmod 25 = ?$	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 duyardi	Xavfsizlik siyosati
293	RSA shifrlash algoritmda 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 (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 $(148 + 14432) \bmod 256$.	244
304	Quyidagi sonlarning eng katta umumiy bo'luvchilarini toping. 88 i 220	44
305	Quyidagi ifodani qiymatini toping. $-17 \bmod 11$	5
306	2 soniga 10 modul bo'yicha teskari sonni toping.	\emptyset
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	Strategiya

	to'plami- ...	
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	Smartkarta 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 qobiliyatini 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 atributlari, 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 atributlari qaysilar?	Foydalanuvchi atributlari, Resurs atributlari, Ob'ekt va muxit atributlari
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 arxitekturasini nechta tashkil etuvchidan iborat?	5
369	WiMAX tarmoq arxitekturasini 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, Trojan 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 printsipligiga 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 xizmatlar/hujumlar/harakatlar bloklanadi
407	Ehtiyotkorlik siyosati (Prudent Policy) – bu	Barcha xizmatlar 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 xizmatlar blokirovka qilingandan so'ng bog'lanadi. Bu qaysi xavfsizlik siyosatiga hos?	Ehtiyotkorlik siyosati (Prudent Policy)
410	Faqat ma'lum xizmatlar/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 arxitekturasini
414	Cloud computing texnologiyasining nechta asosiy turi mavjud?	3
415	Raqamli soatlar qaysi texnologiyaga tegishli?	O'rnatilgan tizimlar (Embedde systems)

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 shifrnı 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, yaxlitlikni 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-funktsiyanı natijasi ...

J: fiksirlangan uzunlikdagi xabar

Ethernet kontsentratori qanday vazifani bajaradi

J: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi

Axborotlarni saqllovchi 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 qoidalarini 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

Shifrtexstni 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 inshonchiligi, 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, garmalash kriptografiyaning qaysi turiga bog'liq?

J: simmetrik kriptosistemalar

Foydalanishni boshqarish –bu...

J: Subyektni Obyektga ishlash qobiliyatini aniqlashdir.

Kompyuterning tashqi interfeysi deganda nima tushuniladi?

J: kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidolari 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 shifratnga 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 haqiqiylikni 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 shifrnı 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 $k_1 \neq k_2$ bo'lib, k_1 ochiq kalit, k_2 yopiq kalit deb yuritiladi, k_1 bilan axborot shifrlanadi, k_2 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

Kriptografiya 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 shifratnga qo'shilgan qo'shimcha

TCP/IP modelida nechta satx mavjud

J: 4

Kriptoanaliz –

J: kalitlarni bilmasdan shifrnı 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

Kriptografiya 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

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 haqiqiylikni 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. Shifrttekstni 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'ektning Ob'ektga ishlash qobiliyatini aniqlashdir.

12. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?

J: Yulduz

13. RSA algoritmi 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