(fanning umumiy soati:*180 c*)

“KIBERXAVFSIZLIK ASOSLARI” FANI

№1 Fan bobi – 1; Bo‘limi – 3; Qiyinchilik darajasi – 1;

CSEC2017 Joint Task Force (CSEC2017 JTF) kiberxavfsizlikka qanday ta’rif bergan?
Kiberxavfsizlik – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlil qilish va testlashni o‘z ichiga oladi.
Kiberxavfsizlik – tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarish, almashtirish yoki yo‘q qilishni; foydalanuvchilardan pul undirishni; yoki normal ish faoliyatini uzub qo‘yishni maqsad qiladi.
Tizim ma’lumoti va axborotiga faqat vakolatga ega sub’ektlar foydalanishi mumkinligini ta’minlovchi qoidalar. Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o‘qilishini” ta’minlaydi.
Ma’lumotni aniq va ishonchli ekanligiga ishonch hosil qilish. Ya’ni, axborotni ruxsat etilmagan o‘zgartirishdan yoki “yozish” dan himoyalash.

№2 Fan bobi – 3; Bo‘limi – 1; Qiyinchilik darajasi – 2;

Tarmoq bo‘yicha faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka qanday ta’rif bergan:
Kiberxavfsizlik – tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarish, almashtirish yoki yo‘q qilishni; foydalanuvchilardan pul undirishni; yoki normal ish faoliyatini uzub qo‘yishni maqsad qiladi.
Kiberxavfsizlik – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlil qilish va testlashni o‘z ichiga oladi.
Tizim ma’lumoti va axborotiga faqat vakolatga ega sub’ektlar foydalanishi mumkinligini ta’minlovchi qoidalar. Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o‘qilishini” ta’minlaydi.
Ma’lumotni aniq va ishonchli ekanligiga ishonch hosil qilish. Ya’ni, axborotni ruxsat etilmagan o‘zgartirishdan yoki “yozish” dan himoyalash.

№3 Fan bobi – 4; Bo‘limi – 2; Qiyinchilik darajasi – 1;

Konfidensiallik bu,
Tizim ma’lumoti va axborotiga faqat vakolatga ega sub’ektlar foydalanishi mumkinligini ta’minlovchi qoidalar. Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o‘qilishini” ta’minlaydi.
Ma’lumotni aniq va ishonchli ekanligiga ishonch hosil qilish. Ya’ni, axborotni ruxsat etilmagan o‘zgartirishdan yoki “yozish” dan himoyalash.
Ma’lumot, axborot va tizimdan foydalanishning mumkinligi. Ya’ni, ruxsat etilmagan “bajarish” dan himoyalash.
Potensial foyda yoki zarar.

№4 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Yaxlitlik (butunlik) bu,
Ma’lumotni aniq va ishonchli ekanligiga ishonch hosil qilish. Ya’ni, axborotni ruxsat etilmagan o‘zgartirishdan yoki “yozish” dan himoyalash.

Tizim ma’lumoti va axborotiga faqat vakolatga ega sub’ektlar foydalanishi mumkinligini ta’minlovchi qoidalar. Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o‘qilishini” ta’minlaydi.
Ma’lumot, axborot va tizimdan foydalanishning mumkinligi. Ya’ni, ruxsat etilmagan “bajarish” dan himoyalash.
Potensial foyda yoki zarar.

№5 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Foydalanuvchanlik bu,
Ma’lumot, axborot va tizimdan foydalanishning mumkinligi. Ya’ni, ruxsat etilmagan “bajarish” dan himoyalash.
Ma’lumotni aniq va ishonchli ekanligiga ishonch hosil qilish. Ya’ni, axborotni ruxsat etilmagan o‘zgartirishdan yoki “yozish” dan himoyalash.
Tizim ma’lumoti va axborotiga faqat vakolatga ega sub’ektlar foydalanishi mumkinligini ta’minlovchi qoidalar. Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o‘qilishini” ta’minlaydi.
Kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarni o‘zaro ta’sirini hisobga oladigan fikrlash jarayoni.

№6 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Risk bu,
potensial foyda yoki zarar.
Ma’lumotni aniq va ishonchli ekanligiga ishonch hosil qilish. Ya’ni, axborotni ruxsat etilmagan o‘zgartirishdan yoki “yozish” dan himoyalash.
Tizim ma’lumoti va axborotiga faqat vakolatga ega sub’ektlar foydalanishi mumkinligini ta’minlovchi qoidalar. Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o‘qilishini” ta’minlaydi.
Ma’lumot, axborot va tizimdan foydalanishning mumkinligi. Ya’ni, ruxsat etilmagan “bajarish” dan himoyalash.

№7 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Hujumchi kabi fikrlash bu,
Bo‘lishi mumkin bo‘lgan xavfni oldini olish uchun qonuniy foydalanuvchini hujumchi kabi fikrlash jarayoni.
Kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarni o‘zaro ta’sirini hisobga oladigan fikrlash jarayoni.
Tizim ma’lumoti va axborotiga faqat vakolatga ega sub’ektlar foydalanishi mumkinligini ta’minlovchi qoidalar. Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o‘qilishini” ta’minlaydi.
Ma’lumot, axborot va tizimdan foydalanishning mumkinligi. Ya’ni, ruxsat etilmagan “bajarish” dan himoyalash.

№8 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Tizimli fikrlash bu,
Kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarni o‘zaro ta’sirini hisobga oladigan fikrlash jarayoni.
Tizim ma’lumoti va axborotiga faqat vakolatga ega sub’ektlar foydalanishi mumkinligini ta’minlovchi qoidalar. Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o‘qilishini” ta’minlaydi.

Ma’lumot, axborot va tizimdan foydalanishning mumkinligi. Ya’ni, ruxsat etilmagan “bajarish” dan himoyalash.
Bo‘lishi mumkin bo‘lgan xavfni oldini olish uchun qonuniy foydalanuvchini hujumchi kabi fikrlash jarayoni.

№9 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Haqiqiy shifrlanmagan ma’lumot bu,
ochiq matn
shifrmatn
deshifrlash
kalit

№10 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Haqiqiy ma’lumotni qayta tiklash jarayoni bu,
deshifrlash
ochiq matn
kalit
kriptoanaliz

№11 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Kodlashtirish bu,
axborotni bir tizimdan boshqa tizimga ma’lum bir belgilar yordamida belgilangan tartib bo‘yicha o‘tkazish jarayoniga aytiladi.
mahfiy xabar mazmunini shifrlash, ya’ni ma’lumotlarni maxsus algoritm bo‘yicha o‘zgartirib, shifrlangan matnni yaratish yo‘li bilan axborotga ruxsat etilmagan kirishga to‘siq qo‘yish usuliga aytiladi.
axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi.
matnni shifrlash va shifrini ochish uchun kerakli axborot.

№12 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Kriptografiya bu,
mahfiy xabar mazmunini shifrlash, ya’ni ma’lumotlarni maxsus algoritm bo‘yicha o‘zgartirib, shifrlangan matnni yaratish yo‘li bilan axborotga ruxsat etilmagan kirishga to‘siq qo‘yish usuliga aytiladi.
axborotni bir tizimdan boshqa tizimga ma’lum bir belgilar yordamida belgilangan tartib bo‘yicha o‘tkazish jarayoniga aytiladi.
kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi.
esa axborotni ikkilik sanoq sistemasidagi “0” va “1” lardan iborat raqamli ko‘rinishidir. Agar axborotni shifrlash va uni qayta tiklash uchun bir xil kalitdan foydalanilsa bunday shifrlash usuli simmetrik shifrlash usuli deyiladi.

№13 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Kalit bu,

matnni shifrlash va shifrini ochish uchun kerakli axborot.
axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi.
kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi.
esa axborotni ikkilik sanoq sistemasidagi “0” va “1” lardan iborat raqamli ko‘rinishidir. Agar axborotni shifrlash va uni qayta tiklash uchun bir xil kalitdan foydalanilsa bunday shifrlash usuli simmetrik shifrlash usuli deyiladi.

№14 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... shifrlarda ma’lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalaniladi.
Cimmetrik
Assimetrik
Elektron raqamli imzo
Vijiner

№15 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... kriptotizimlarda shifrlash va deshifrlash uchun turlicha kalitlardan foydalaniladi.
Assimetrik
Simmetrik
Elektron raqamli imzo
Xesh funksiya

№16 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... bu maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi.
Stenanografiya
Kriptografiya
Kriptoanaliz
Xesh funksiya

№17 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... da esa jo‘natuvchi faqat ochiq matn ko‘rinishidagi xabar yuborishi mumkin, bunda u xabarni ochiq tarmoq (masalan, Internet) orqali uzatishdan oldin shifrlangan matnga o‘zgartiradi.
Kriptografiya
Kriptoanaliz
Xesh funksiya
Ctenanografiya

№18 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... shifrlash usuli bo‘yicha boshlang‘ich matn belgilarining matnning ma’lum bir qismi doirasida maxsus qoidalar yordamida o‘rinlari almashtiriladi.
O‘rinlarini almashtirish

Taxliliy o‘zgartirish
Gammalashtirish
Almashtirish

№19 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... shifrlash usuli bo‘yicha boshlang‘ich matn belgilari foydalanilayotgan yoki boshqa bir alifbo belgilariga almashtiriladi.
Almashtirish
O‘rinlarini almashtirish
Taxliliy o‘zgartirish
Gammalashtirish

№20 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... usuli bo‘yicha boshlang‘ich matn belgilari shifrlash gammasi belgilari, ya’ni tasodifiy belgilar ketma-ketligi bilan birlashtiriladi.
Gammalashtirish
Almashtirish
O‘rinlarini almashtirish
Taxliliy o‘zgartirish

№21 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... usuli bo‘yicha boshlang‘ich matn belgilari analitik formulalar yordamida o‘zgartiriladi, masalan, vektorni matritsaga ko‘paytirish yordamida. Bu yerda vektor matndagi belgilar ketma-ketligi bo‘lsa, matritsa esa kalit sifatida xizmat qiladi.
Taxliliy o‘zgartirish
Gammalashtirish
Almashtirish
O‘rinlarini almashtirish

№22 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Shifrlashning qaysi usullariga binoan dastlabki axborot simvollariga mos keluvchi raqam kodlarini ketma-ketligi gamma deb ataluvchi qandaydir simvollar ketma-ketligiga mos keluvchi kodlar ketma-ketligi bilan ketma-ket jamlanadi.
Additiv
Kombinatsiyalangan
Almashtirish
O‘rinlarini almashtirish

№23 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Ushbu standart — kriptografik algoritm, elektron ma’lumotlarni himoyalashga mo‘ljallangan.
Ma’lumotlarni shifrlash algoritmi

DES
SHA
El-gamal

№24 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Asimmetrik shifrlashning birinchi va keng tarqalgan kriptoalgoritmi .....1993 yilda standart sifatida qabul qilindi.
RSA
DES
SHA
El-gamal

№25 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Elektron raqamli imzo tizimi ikkita asosiy muolajani amalga oshiradi:
raqamli imzoni shakllantirish muolajasi, raqamli imzoni tekshirish muolajasi
raqamli imzoni tekshirish muolajasi, raqamli imzoni buzish muolajasi
raqamli imzoni shakllantirish muolajasi, raqamli imzoni kolliziyaga tekshirish muolajasi
raqamli imzoni kolliziyaga tekshirish muolajasi, raqamli imzoni tekshirish muolajasi

№26 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

1977 yilda AQSh da yaratilgan ..... birinchi va dunyoda mashhur elektron raqamli imzo tizimi hisoblanadi.
RSA tizimi
DES tizimi
SHA tizimi
El-gamal tizimi

№27 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Ishonchliligining yuqoriligi va shaxsiy kompyuterlarda amalga oshirilishining qulayligi bilan ajralib turuvchi raqamli imzo algoritmli 1984 yilda ..... tomonidan ishlab chiqildi.
El-Gamal
Raman
Shamil
Adelman

№28 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Kriptologiya bu,
Maxfiy kodlarni yaratish va buzish fani va san’ati
Maxfiy kodlarni yaratish bilan shug‘ullanadi
Maxfiy kodlarni buzish bilan shug‘ullanadi

Maxfiy kodlarni analitik tahlili bilan shug‘ullanadi

№29 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Kriptografiya bu,
Maxfiy kodlarni yaratish bilan shug‘ullanadi
Maxfiy kodlarni buzish bilan shug‘ullanadi
Maxfiy kodlarni analitik tahlili bilan shug‘ullanadi
Maxfiy kodlarni yaratish va buzish fani va san’ati

№30 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Kriptotahlil bu,
Maxfiy kodlarni buzish bilan shug‘ullanadi
Maxfiy kodlarni analitik tahlili bilan shug‘ullanadi
Maxfiy kodlarni yaratish va buzish fani va san’ati
Maxfiy kodlarni yaratish bilan shug‘ullanadi

№31 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... ma’lumotni osongina qaytarish uchun hammaga (hattoki hujumchiga ham) ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir.
Kodlash
Shifrlash
Steganografiya
Watermarking

№32 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... ma’lumotlardan foydalanish qulayligini ta’minlash uchun amalga oshiriladi va hammaga ochiq bo‘lgan sxemalardan foydalaniladi.
Kodlash
Shifrlash
Steganografiya
Watermarking

№33 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... jarayonida ham ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar (deshifrlash kalitiga ega bo‘lgan) qayta o‘zgartirishi mumkin bo‘ladi.
Shifrlash
Steganografiya
Watermarking
Kodlash

№34 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

.....dan asosiy maqsad ma’lumotni maxfiyligini ta’minlash bo‘lib, uni qayta o‘zgartirish ba’zi shaxslar (deshifrlash kalitiga ega bo‘lgan) qayta o‘zgartirishi mumkin bo‘ladi.
Shifrlash
Steganografiya
Watermarking
Kodlash

№35 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... bu maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi.
Stenanografiya
Shifrlash
Watermarking
Kodlash

№36 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

.....ning asosiy g‘oyasi bu – bu maxfiy ma’lumotlarning mavjudligi haqidagi shubhani oldini olish hisoblanadi.
Stenanografiya
Shifrlash
Watermarking
Kodlash

№37 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

.....dan asosiy maqsad ma’lumotni maxfiyligini qolganlardan sir tutishdir.
Shifrlash
Steganografiya
Watermarking
Kodlash

№38 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Simmetrik kalitli kriptotizimlar bu,
Bir kalitli kriptotizimlar
Ko‘p kalitli kriptotizimlar
Assimmetrik kriptotizimlar
Xesh funksiyalar

№39 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Ochiq kalitli kriptotizimlar bu,
Ikki kalitli kriptotizimlar
Bir kalitli kriptotizimlar
Ko‘p kalitli kriptotizimlar
Assimmetrik kriptotizimlar

№40 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Ma’lumotni ..... uning butunligini kafolatlash maqsadida amalga oshiriladi.
Xeshlash
Kodlash
Shifrlash
Deshifrlash

№41 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... da odatda kiruvchi ma’lumotning uzunligi o‘zgaruvchan bo‘lib, chiqishda o‘zgarmas uzunlikdagi qiymatni qaytaradi.
Xesh funksiya
Kodlash
Shifrlash
Stenanografiya

№42 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Odatda xesh funksiyalar kirishda ma’lumotdan tashqari hech qanday qiymatni talab etmagani bois ..... deb ham ataladi.
Kalitsiz kriptografik funksiyalar
Kalitli kriptografik funksiyalar
Elektron raqamli imzo (ERI) algoritmlari
Gamilton algoritmlari

№43 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Qadimgi davr klassik shifrlari keltirilgan javoblarni belgilang.
Sezar, polibiya kvadrati
Vijiner, atbash
Zimmerman telegrami, enigma shifri, SIGABA mashinalari
DES, AES, IDEA, RC4

№44 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

O‘rta davr klassik shifrlari keltirilgan javoblarni belgilang.
Vijiner, atbash

Zimmerman telegrami, enigma shifri, SIGABA mashinalari
DES, AES, IDEA, RC4
Sezar, polibiya kvadrati

№45 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

1 va 2-jahon urushi davri klassik shifrlari keltirilgan javoblarni belgilang.
Zimmerman telegrami, enigma shifri, SIGABA mashinalari
DES, AES, IDEA, RC4
Sezar, polibiya kvadrati
Vijiner, atbash

№46 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Zamonaviy shifrlar keltirilgan javoblarni belgilang.
DES, AES, IDEA, RC4
Sezar, polibiya kvadrati
Vijiner, atbash
Zimmerman telegrami, enigma shifri, SIGABA mashinalari

№47 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... shifri nomi bilan tanilgan kriptotizim bardoshli shifrlash algoritmi hisoblanadi.
Bir martali bloknot yoki vernam
Vijiner
Atbash
Polibiya kvadrati

№48 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Bir martali bloknot usulida ochiq matnga kalitni ..... amalida qo‘shish orqali shifrmatn hosil qilinadi.
XOR
OR
NOT
MOD

№49 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Kodlar kitobi orqali mashhur ..... shifrlangan.
Zimmermann telegrami
SIGABA mashinasi
Enigma shifri

GOST 34791 standarti

№50 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Kodlar kitobi asosida shifrlash ..... akslantirishiga asoslangan.
O‘rniga qo‘yish
Gammalashtirish
Almashtirish
Tahliliy o‘zgartirish

№51 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... hozirda amalda qo‘llaniluvchi simmetrik blokli shifrlarni yaratishga asos bo‘lgan.
Kodlar kitobi
Bir martali bloknot
Gammalashtirish
Tahliliy o‘zgartirish

№52 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... o‘z davrida yetarli xavfsizlikni ta’minlagan shifrlash usuli hisoblanadi.
Kodlar kitobi
Bir martali bloknot
Gammalashtirish
Tahliliy o‘zgartirish

№53 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... kriptotizimlarda ma’lumotni shifrlashda va deshifrlashda yagona kalitdan foydalaniladi.
Simmetrik
Assimmetrik
Affin
Xesh funksiya

№54 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Simmetrik kriptotizimlar 2 guruhga ajratiladi:
Simmetrik oqimli shifrlar, simmetrik blokli shifrlar
Simmetrik oqimli shifrlar, assimmetrik blokli shifrlar
Assimmetrik oqimli shifrlar, simmetrik blokli shifrlar
Assimmetrik oqimli shifrlar, assimmetrik blokli shifrlar

№55 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

7mod3=?
1
2
0
3

№56 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

14mod3=?
2
1
3
0

№57 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

2mod3=?
2
1
3
0

№58 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

-7mod3=?
2
1
0
3

№59 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

-2mod5=?
3
0
1
2

№60 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

RSA ochiq kalitli shifrlash algoritmi mualliflari ..... bo‘lgan uchta olim sharafiga qo‘yilgan.
Rivest, Shamir, Adleman
Ravir, Shamir, Adelman

Riavir, Shanel, Adleman
Rivest, Shamer, Adelman

№61 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

RSA algoritmi katta sonlarni ..... ga asoslanadi.
Faktorlash muammosi
Generatsiyalash
Tub ko‘paytuvchilarga ajratish
Qoldiq

№62 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

RSA algoritmida quyidagi jarayonlar mavjud:
Kalitni generatsiyalash, shifrlash, deshifrlash
Kalitni generatsiyalash, shifrlash, qoldiq
Kalitni generatsiyalash, deshifrlash, qoldiq
Shifrlash, deshifrlash, qoldiq

№63 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Xesh qiymat M ma’lumot uchun qanday ko‘rinishda hisoblanadi?
h(M)
H(M)
(M)
h(m)

№64 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

MAC bu,
Message authentication code
Message authentication computer
Message avtorization code
Message avtorization computer

№65 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

MAC bu,
Xabarlarni autentifikatsiyalash kodi
Xabarlarni avtorizatsiyalash kompyuteri
Xabarlarni avtorizatsiyalash kodi
Xabarlarni avtorizatsiyalash kompyuteri

№66 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Elektron raqamli imzo (ERI) bu,
Elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgartirish natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo.
Elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgartirish natijasida hosil qilingan hamda elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo.
Elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgartirish natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash imkoniyatini beradigan imzo.
Elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgartirish va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo.

№67 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

PKI bu,
Public key infrastructure
Public key international
Public kase international
Public kase infrastructure

№68 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

PKI bu,
Ochiq kalitlar infratuzilmasi
Ochiq kalitlar birligi
Ochiq kalitlar guruhi
Ochiq kalitlar innovatsiyasi

№69 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

SA bu,
Certificate authorit
Certificate authentication
Certificate avtorization
Certificate identification

№70 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

SA bu,
Sertifikat markazi
Sertifikat autentifikatsiyasi

Sertifikat avtorizatsiyasi
Sertifikat identifikatsiyasi

№71 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Raqamli sertifikat bu,
Ochiq kalit sertifikati
Yopiq kalit sertifikati
Sertifikatlar byurosi
Setifikatlar markazi

№72 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Raqamli sertifikat bu,
Qisqacha sertifikat
Yopiq kalit sertifikati
Sertifikatlar byurosi
Setifikatlar markazi

№73 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... foydalanuvchining ismi va uning ochiq kalitidan iborat bo‘ladi.
Raqamli sertifikat
Yopiq kalit sertifikati
Sertifikatlar byurosi
Setifikatlar markazi

№74 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... odatda tomoni odatda uchinchi tomon (trusted third party yoki TTP) sifatida qaraladi.
Certificate authorit (CA)
Certificate authentication (CA)
Certificate avtorization (CA)
Certificate identification (CI)

№75 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Ruxsatlarni nazoratlash sohasi quyidagi qism sohalardan iborat:
Identifikatsiya, autentifikatsiya, avtorizatsiya
Identifikatsiya, autentifikatsiya, ma’murlash
Identifikatsiya, avtorizatsiya, ma’murlash
autentifikatsiya, avtorizatsiya, ma’murlash

№76 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... shaxsni kimdir deb davo qilish jarayoni.
Identifikatsiya
Autentifikatsiya
Avtorizatsiya
Ma’murlash

№77 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

“Men Bahodirman” identifikatorni toping.
Bahodir
Men
Men Bahodirman
Bu yerda identifikator ko‘rsatilmagan

№78 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim etish jarayoni.
Identifikatsiya
Autentifikatsiya
Avtorizatsiya
Ma’murlash

№79 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni.
Autentifikatsiya
Avtorizatsiya
Ma’murlash
Identifikatsiya

№80 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... foydalanuvchi yoki sub’ektni haqiqiyligini tekshirish jarayoni.
Autentifikatsiya
Avtorizatsiya
Ma’murlash
Identifikatsiya

№81 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayonidir.

Avtorizatsiya
Ma’murlash
Identifikatsiya
Autentifikatsiya

№82 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... binar qaror – ya’ni, ruxsat beriladi yoki yo‘q.
Autentifikatsiya
Ma’murlash
Identifikatsiya
Avtorizatsiya

№83 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... esa tizimning turli resurslariga foydalanishni cheklash uchun foydalanuvchi qoidalar to‘plami haqidagi barcha narsa.
Avtorizatsiya
Ma’murlash
Identifikatsiya
Autentifikatsiya

№84 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... siz kimsiz?
Identifikatsiya
Autentifikatsiya
Avtorizatsiya
Ma’murlash

№85 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... siz haqiqatdan ham sizmisiz?
Autentifikatsiya
Ma’murlash
Identifikatsiya
Avtorizatsiya

№86 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... sizga buni bajarishga ruxsat bormi?
Avtorizatsiya
Ma’murlash

Identifikatsiya
Autentifikatsiya

№87 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot.
Parol
Smartkarta
Token
Kalit

№88 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... kredit karta o‘lchamidagi qurilma bo‘lib, kichik hajmdagi xotira va hisoblash imkoniyatiga ega.
Smartkarta
Token
Kalit
Parol

№89 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Biometrik parametrlar insonning o‘zi uchun ..... kalit sifatida xizmat qiladi.
Kalit
Parol
Smartkarta
Token

№90 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... biometrik parametr barcha foydalanuvchilarda bo‘lishi shart.
Universal bo‘lishi
Farqli bo‘lish
O‘zgarmaslik
To‘planuvchanlik

№91 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... tanlangan biometrik parametr barcha insonlar uchun farq qilishi shart.
Farqli bo‘lish
O‘zgarmaslik
To‘planuvchanlik
Universal bo‘lishi

№92 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... tanlangan biometrik parametr vaqt o‘tishi bilan o‘zgarmay qolishi shart.
O‘zgarmaslik
To‘planuvchanlik
Universal bo‘lishi
Farqli bo‘lish

№93 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... fizik xususiyat osonlik bilan to‘planuvchi bo‘lishi shart. Amalda fizik xususiyatni to‘planuvchanligi, insonning jarayonga e’tibor berishiga ham bog‘liq bo‘ladi.
To‘planuvchanlik
Universal bo‘lishi
Farqli bo‘lish
O‘zgarmaslik

№94 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Agar tomonlardan biri ikkinchisini autentifikatsiyadan o‘tkazsa, ... deb ataladi.
Bir tomonlama autentifikatsiya
Ikki tomonlama autentifikatsiya
Bir faktorli autentifikatsiya
Ko‘p faktorli autentifikatsiya

№95 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

“Elektron pochtadan foydalanish davomida faqat server foydalanuvchini haqiqiyligini tekshiradi” qaysi turdagi autentifikatsiya.
Bir tomonlama autentifikatsiya
Ikki tomonlama autentifikatsiya
Bir faktorli autentifikatsiya
Ko‘p faktorli autentifikatsiya

№96 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Agar har ikkala tomon bir-birini autentifikatsiyadan o‘tkazsa, u holda ..... deb ataladi.
Ikki tomonlama autentifikatsiya
Bir faktorli autentifikatsiya
Ko‘p faktorli autentifikatsiya
Bir tomonlama autentifikatsiya

№97 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

“Elektron to‘lovlarni amalga oshirishda esa ham server foydalanuvchini autentifikatsiyadan

o‘tkazadi ham foydalanuvchi serverni autentifikatsiyadan o‘tkazadi” qaysi turdagi autentifikatsiya.
Ikki tomonlama autentifikatsiya
Bir faktorli autentifikatsiya
Ko‘p faktorli autentifikatsiya
Bir tomonlama autentifikatsiya

№98 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Pochtaga kirishda faqat parolni bilsangiz siz autentifikatsiyadan o‘ta olasiz. Bu qaysi turdagi autentifikatsiya.
Bir faktorli autentifikatsiya
Ko‘p faktorli autentifikatsiya
Bir tomonlama autentifikatsiya
Ikki tomonlama autentifikatsiya

№99 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Tekshirish faqat bitta faktor bo‘yicha (masalan parol) amalga oshiriladi. Bu qaysi turdagi autentifikatsiya.
Bir faktorli autentifikatsiya
Ko‘p faktorli autentifikatsiya
Bir tomonlama autentifikatsiya
Ikki tomonlama autentifikatsiya

№100 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Mazkur muammoni bartaraf etish uchun, birinchi faktorga qo‘shimcha qilib, yana boshqa faktorlardan foydalanish mumkin. Bu qaysi turdagi autentifikatsiya.
Ko‘p faktorli autentifikatsiya
Bir tomonlama autentifikatsiya
Ikki tomonlama autentifikatsiya
Bir faktorli autentifikatsiya

№101 Fan bobi – 2; Bo‘limi – 3; Qiyinchilik darajasi – 1;

Ovozga asoslangan autentifikatsiyalashda qo‘shimcha qilib paroldan foydalanish mumkin. Bu qaysi turdagi autentifikatsiya.
Ko‘p faktorli autentifikatsiya
Bir tomonlama autentifikatsiya
Ikki tomonlama autentifikatsiya
Bir faktorli autentifikatsiya

№102 Fan bobi – 3; Bo‘limi – 1; Qiyinchilik darajasi – 2;

Foydalanuvchi dastlab tizimga o‘z ovozi orqali autentifikatsiyadan o‘tadi va undan so‘ng parol bo‘yicha autentifikatsiyadan o‘tkaziladi. Bu qaysi turdagi autentifikatsiya.
Ko‘p faktorli autentifikatsiya

Bir tomonlama autentifikatsiya
Ikki tomonlama autentifikatsiya
Bir faktorli autentifikatsiya

№103 Fan bobi – 4; Bo‘limi – 2; Qiyinchilik darajasi – 1;

Plastik kartadan to‘lovni amalga oshirishdagi autentifikatsiya.
Ko‘p faktorli autentifikatsiya
Bir tomonlama autentifikatsiya
Ikki tomonlama autentifikatsiya
Bir faktorli autentifikatsiya

№104 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Dastlab foydalanuvchida plastik kartani o‘zini bor bo‘lishini talab etadi va ikkinchidan uni PIN kodini bilishni talab etadi. Bu qaysi turdagi autentifikatsiya.
Ko‘p faktorli autentifikatsiya
Bir tomonlama autentifikatsiya
Ikki tomonlama autentifikatsiya
Bir faktorli autentifikatsiya

№105 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... usuli faktorlardan bittasi qalbakilashtirilgan taqdirda ham autentifikatsiya jarayonini buzilmasligiga olib keladi.
Ko‘p faktorli autentifikatsiya
Bir tomonlama autentifikatsiya
Ikki tomonlama autentifikatsiya
Bir faktorli autentifikatsiya

№106 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... faqat bir marta foydalanuvchi parol bo‘lib, har bir sessiya uchun o‘zgarib turadi.
One time password (OTP)
Smartkarta
Token
Kalit

№107 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Turli mobayl ilovalarida to‘lovlarni amalga oshirishda SMS xabar ko‘rinishida ..... lar kelishi mumkin.
One time password (OTP)
Smartkarta

Token
Kalit

№108 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... ga asoslangan autentifikatsiya oddiy statik parolga qaraganda yuqori xavfsizlik darajasiga ega.
One time password (OTP)
Smartkarta
Token
Kalit

№109 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... odatda ikkinchi faktor sifatida foydalaniladi.
One time password (OTP)
Smartkarta
Token
Kalit

№110 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Vaqtni sinxronlashga asoslangan dasturiy OTP generatori bu,
Google Authenticator
Smartkarta
Token
Certificate authenticator

№111 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Hujumning mazkur turi tokenni yoki smart kartani o‘g‘irlashni maqsad qiladi. Bu,
Fizik o‘g‘irlash
Qalbakilashtirish
Dasturiy ko‘rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
Ma’lumotlar bazasidagi biometrik parametrlarni almashtirish

№112 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Ba’zi tokenlar dasturiy ko‘rinishda bo‘lib, mobil qurilmalarda ishlaydi va shu sababli zararli dastur tomonidan boshqarilishi mumkin. Bu,
Dasturiy ko‘rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
Ma’lumotlar bazasidagi biometrik parametrlarni almashtirish
Fizik o‘g‘irlash
Qalbakilashtirish

№113 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Yuzlari o‘xshash bo‘lgan Hasan o‘rniga Husan autentifikatsiyadan o‘tishi bu,
Qalbakilashtirish
Dasturiy ko‘rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
Ma’lumotlar bazasidagi biometrik parametrlarni almashtirish
Fizik o‘g‘irlash

№114 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Sifati yuqori bo‘lgan foydalanuvchi yuz tasviri mavjud rasm bilan tizimni aldashi bu,
Qalbakilashtirish
Dasturiy ko‘rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
Ma’lumotlar bazasidagi biometrik parametrlarni almashtirish
Fizik o‘g‘irlash

№115 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Ushbu hujum bevosita foydalanuvchilarni biometrik parametrlari saqlangan bazaga qarshi amalga oshiriladi.
Ma’lumotlar bazasidagi biometrik parametrlarni almashtirish
Qalbakilashtirish
Dasturiy ko‘rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
Fizik o‘g‘irlash

№116 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Ushbu hujumda tanlangan foydalanuvchini biometrik parametrlari hujumchini biometrik parametrlari bilan almashtiriladi.
Ma’lumotlar bazasidagi biometrik parametrlarni almashtirish
Qalbakilashtirish
Dasturiy ko‘rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
Fizik o‘g‘irlash

№117 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Mashhur parolni buzuvchi vositalar:
Password Crackers, Password Portal, L0phtCrack and LC4, John the Ripper
Password Crackers, Antivitask manager, Avast
Doctor web, Antivitask manager, Avast
Doctor web, eset nod, Avast

№118 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Adminlar ushbu vositalardan foydalanish orqali parollarni tekshirish zarar, bular
Password Crackers, Password Portal, L0phtCrack and LC4, John the Ripper
Password Crackers, Antivitask manager, Avast
Doctor web, Antivitask manager, Avast
Doctor web, eset nod, Avast

№119 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Tabiiy tahdidlarni ko‘rsating:
Toshqinlar, yong‘inlar, zilzila, harorat va namlik
Vandalizm, qurilmaning yoqolishi, fizik qurilmalarning buzilishi, o‘g‘irlash, sotsial injeneriya, tizimlarni ruxsat etilmagan nazoratlash
Vandalizm, qurilmaning yoqolishi, zilzila, harorat va namlik
Toshqinlar, yong‘inlar, fizik qurilmalarning buzilishi, o‘g‘irlash

№120 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Sun’iy tahdidlarni ko‘rsating:
Vandalizm, qurilmaning yoqolishi, fizik qurilmalarning buzilishi, o‘g‘irlash, sotsial injeneriya, tizimlarni ruxsat etilmagan nazoratlash
Vandalizm, qurilmaning yoqolishi, zilzila, harorat va namlik
Toshqinlar, yong‘inlar, fizik qurilmalarning buzilishi, o‘g‘irlash
Toshqinlar, yong‘inlar, zilzila, harorat va namlik

№121 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Fizik xavfsizlikni nazoratlash tashkilot axborot aktivlarini va binolaridan foydalanishni ..... ga yordam beradi.
Kuzatish, qaydlash, nazoratlash
Ma’muriy nazorat, qaydlash, nazoratlash
Kuzatish, qaydlash, fizik nazorat
Kuzatish, ma’muriy nazorat, fizik nazorat

№122 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Ma’muriy nazorat bu,
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik belgilari va ogohlantirish signallari, ishchi joy xavfsizligini ta’minlash, shaxs xavfsizligini ta’minlash
Fizik to‘siqlarni o‘rnatish, xavfsizlik qo‘riqchilarini ishga olish, fizik qulflar
Ruxsatlarni nazoratlash, “qopqon”, yong‘inga qarshi tizimlar, yoritish tizimlari, ogohlantirish tizimlari, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik qo‘riqchilarini ishga olish, fizik qulflar, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash

№123 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Fizik nazorat bu,
Fizik to‘siqlarni o‘rnatish, xavfsizlik qo‘riqchilarini ishgа olish, fizik qulflar
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik belgilari va ogohlantirish signallari, ishchi joy xavfsizligini ta’minlash, shaxs xavfsizligini ta’minlash
Ruxsatlarni nazoratlash, “qopqon”, yong‘inga qarshi tizimlar, yoritish tizimlari, ogohlantirish tizimlari, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik qo‘riqchilarini ishgа olish, fizik qulflar, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash

№124 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Texnik nazorat bu,
Ruxsatlarni nazoratlash, “qopqon”, yong‘inga qarshi tizimlar, yoritish tizimlari, ogohlantirish tizimlari, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik qo‘riqchilarini ishgа olish, fizik qulflar, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik belgilari va ogohlantirish signallari, ishchi joy xavfsizligini ta’minlash, shaxs xavfsizligini ta’minlash
Fizik to‘siqlarni o‘rnatish, xavfsizlik qo‘riqchilarini ishgа olish, fizik qulflar

№125 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... sub’ektni ob’ektga ishlash qobiliyatini aniqlash.
Foydalanishni boshqarish
Sub’ekt
Ob’ekt
Ma’murlash

№126 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... bu inson, dastur, jarayon va hokazo bo‘lishi mumkin.
Sub’ekt
Ob’ekt
Ma’murlash
Foydalanishni boshqarish

№127 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... bu ma’lumot, resurs, jarayon va hokazo bo‘lishi mumkin.
Ob’ekt
Ma’murlash
Foydalanishni boshqarish

Sub’ekt

№128 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

DAC (Discretionary access control) bu,
Diskresion foydalanishni boshqarish usuli
Mandatli foydalanishni boshqarish usuli
Rolga asoslangan foydalanishni boshqarish usuli
Atributlarga asoslangan foydalanishni boshqarish usuli

№129 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

MAC (Mandatory access control) bu,
Mandatli foydalanishni boshqarish usuli
Rolga asoslangan foydalanishni boshqarish usuli
Atributlarga asoslangan foydalanishni boshqarish usuli
Diskresion foydalanishni boshqarish usuli

№130 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

RBAC (Role-based access control) bu,
Rolga asoslangan foydalanishni boshqarish usuli
Atributlarga asoslangan foydalanishni boshqarish usuli
Diskresion foydalanishni boshqarish usuli
Mandatli foydalanishni boshqarish usuli

№131 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

ABAC (Attribute-based access control) bu,
Atributlarga asoslangan foydalanishni boshqarish usuli
Diskresion foydalanishni boshqarish usuli
Mandatli foydalanishni boshqarish usuli
Rolga asoslangan foydalanishni boshqarish usuli

№132 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Foydalanishni boshqarishning mazkur usuli tizimdagi shaxsiy ob’ektlarni himoyalash uchun qo‘llaniladi. Bu,
DAC usuli
MAC usuli
RBAC usuli
ABAC usuli

№133 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Bu usulga ko‘ra ob’ekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi.
DAC usuli
MAC usuli
RBAC usuli
ABAC usuli

№134 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... da sub’ektlar tomonidan ob’ektlarni boshqarish sub’ektlarning identifikatsiya axborotiga asoslanadi.
DAC usuli
MAC usuli
RBAC usuli
ABAC usuli

№135 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

UNIX operatsion tizimida fayllarni himoyalashda, fayl egasi qolganlarga o‘qish (r), yozish (w) va bajarish (x) amallaridan bir yoki bir nechtasini berishi mumkin. Bu qaysi usul?
DAC usuli
MAC usuli
RBAC usuli
ABAC usuli

№136 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... da ob’ektning egasi xavfsizlik siyosatini quradi va kimga foydalanish uchun ruxsat berilishini aniqlaydi.
DAC usuli
MAC usuli
RBAC usuli
ABAC usuli

№137 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... da foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi.
MAC usuli
RBAC usuli
ABAC usuli
DAC usuli

№138 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Ushbu usulda tizimning har bir sub’ekti va ob’ekti bir nechta xavfsizlik darajasiga ega bo‘ladi.
MAC usuli
RBAC usuli
ABAC usuli
DAC usuli

№139 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Ushbu usulda ob’ektning xavfsizlik darajasi tashkilotda ob’ektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi.
MAC usuli
RBAC usuli
ABAC usuli
DAC usuli

№140 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Ushbu usulda sub’ektning xavfsizlik darajasi unga ishonish darajasi bilan belgilanadi.
MAC usuli
RBAC usuli
ABAC usuli
DAC usuli

№141 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda xavfsizlik siyosati ma’muri tomonidan amalga oshiriladi.
MAC usuli
RBAC usuli
ABAC usuli
DAC usuli

№142 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... o‘rnatilgan tizimlar xavfsizlik siyosati ma’muriga tashkilot bo‘ylab xavfsizlik siyosatini amalga oshirish imkoniyatini beradi.
MAC usuli
RBAC usuli
ABAC usuli
DAC usuli

№143 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... da foydalanishni boshqarishning asosiy g‘oyasi tizimning ishlash logikasini tashkilotda kadrlar vazifasiga yaqinlashtirish.

RBAC usuli
ABAC usuli
DAC usuli
MAC usuli

№144 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... da har bir ob’ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun ob’ektlardan foydalanish ruxsatini ko‘rsatish yetarli.
RBAC usuli
ABAC usuli
DAC usuli
MAC usuli

№145 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... da foydalanuvchilar o‘z navbatida o‘zlarining rollarini ko‘rsatishadi.
RBAC usuli
ABAC usuli
DAC usuli
MAC usuli

№146 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... 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 usuli
DAC usuli
MAC usuli
RBAC usuli

№147 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Avtorizatsiyaning klassik ko‘rinishi ..... ning foydalanishni boshqarish matritsasidan boshlanadi.
Lampson
Rivest
Shamir
Adlemann

№148 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

ACL (Access control list) bu,

Foydalanishni boshqarish ro‘yxati
Imtiyozlar ro‘yxati
Foydalanishni boshqarish matritsasi
Sertifikat markazi

№149 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

C-list (Capability list) bu,
Imtiyozlar ro‘yxati
Foydalanishni boshqarish matritsasi
Sertifikat markazi
Foydalanishni boshqarish ro‘yxati

№150 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Tartibsiz yordamchi bu,
Ko‘p jabhalarda klassik xavfsizlik muammosi hisoblanadi
Ko‘p jabhalarda klassik xavfsizlik muammosi hisoblanmaydi
Zamonaviy xavfsizlik muammosi hisoblanmaydi
Zamonaviy xavfsizlik muammosi hisoblanadi

№151 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... bir-biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan komp’yuterlar guruhi.
Komp’yuter tarmoqlari
Internet
Protokol
Intranet

№152 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir.
Tarmoq modeli
Internet
Protokol
Intranet

№153 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

..... modeli tarmoq bo‘ylab ma’lumotlar almashinuvini aniqlashtirish uchun taqdim etilgan model.
OSI
OTP

TCP
IP

№154 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Fizik sath vazifasi:
Qurilma, signal va binar o‘zgartirishlar
Fizik manzillash
Yo‘lni aniqlash va mantiqiy manzillash
Nuqta-nuqta ulanish, ishonchlilik va oqimni nazoratlash

№155 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Kanal sath vazifasi:
Fizik manzillash
Yo‘lni aniqlash va mantiqiy manzillash
Nuqta-nuqta ulanish, ishonchlilik va oqimni nazoratlash
Qurilma, signal va binar o‘zgartirishlar

№156 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Tarmoq sath vazifasi:
Yo‘lni aniqlash va mantiqiy manzillash
Nuqta-nuqta ulanish, ishonchlilik va oqimni nazoratlash
Qurilma, signal va binar o‘zgartirishlar
Fizik manzillash

№157 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Transport sath vazifasi:
Nuqta-nuqta ulanish, ishonchlilik va oqimni nazoratlash
Qurilma, signal va binar o‘zgartirishlar
Fizik manzillash
Yo‘lni aniqlash va mantiqiy manzillash

№158 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Seans sath vazifasi:
Host osti ulanish, ilovalar orasida ulanishlarni boshqarish
Qurilma, signal va binar o‘zgartirishlar
Fizik manzillash
Yo‘lni aniqlash va mantiqiy manzillash

№159 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Taqdimot sath vazifasi:
Ma’lumotni taqdim etish, shifrlash va deshifrlash, mashinaga mos tilga o‘girish va teskarisi
Host osti ulanish, ilovalar orasida ulanishlarni boshqarish
Qurilma, signal va binar o‘zgartirishlar
Fizik manzillash

№160 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Ilova sathi vazifasi:
Ilovalarni tarmoqqa ulanish jarayoni
Ma’lumotni taqdim etish, shifrlash va deshifrlash, mashinaga mos tilga o‘girish va teskarisi
Host osti ulanish, ilovalar orasida ulanishlarni boshqarish
Qurilma, signal va binar o‘zgartirishlar

№161 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

“Yuqori sath protokollarini o‘zida saqlaydi, taqdim etish, kodlash va muloqotni nazoratlash”, qaysi sath vazifasi?
Ilova sathi
Transport sathi
Tarmoq sathi
Kanal sathi

№162 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

“Tomonlar orasida mantiqiy ulanishni o‘rnatadi va transport xizmatini ta’minlaydi”, bu qaysi sath vazifasi?
Transport sathi
Tarmoq sathi
Kanal sathi
Ilova sathi

№163 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

“Manba tarmoqdan masofadagi tarmoqga ma’lumotlarni uzatish bilan tarmoqlararo paket almashinuvini amalga oshiradi”, bu qaysi sath vazifasi?
Tarmoq sathi
Kanal sathi
Ilova sathi
Transport sathi

№164 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

“Bir xil tarmoqda ikkita hostlar orasida Internet sathi bo‘ylab ma’lumot oqishini ta’minlaydi”, bu qaysi sath vazifasi?
Kanal sathi
Ilova sathi
Transport sathi
Tarmoq sathi

№165 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Ilova sathi protokollarini ko‘rsating?
HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP
TCP, UDP, RTP
IP, ICMP, ARP, RARP
Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232

№166 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Transport sathi protokollarini ko‘rsating?
TCP, UDP, RTP
IP, ICMP, ARP, RARP
Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232
HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP

№167 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Tarmoq sathi protokollarini ko‘rsating?
IP, ICMP, ARP, RARP
Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232
HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP
TCP, UDP, RTP

№168 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Kanal sathi protokollarini ko‘rsating?
Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232
HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP
TCP, UDP, RTP
IP, ICMP, ARP, RARP

№169 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Tahdid bu,
Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi va ularni uzib

qo‘yuvchi oshkor bo‘lmagan hodisalarning potensial paydo bo‘lishidir.
Portlaganida tizim xavfsizligini buzuvchi kutilmagan va oshkor bo‘lmagan hodisalarga olib keluvchi kamchilik, loyihalashdagi yoki amalga oshirishdagi xatolik.
Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat.
Ishdan bo‘shab ketgan xodim taqsimlangan diskdan haligacha foydalanish imkoniyatiga ega bo‘lishi mumkinligi.

№170 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Zaiflik bu,
Portlaganida tizim xavfsizligini buzuvchi kutilmagan va oshkor bo‘lmagan hodisalarga olib keluvchi kamchilik, loyihalashdagi yoki amalga oshirishdagi xatolik.
Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat.
Ishdan bo‘shab ketgan xodim taqsimlangan diskdan haligacha foydalanish imkoniyatiga ega bo‘lishi mumkinligi.
Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi va ularni uzib qo‘yuvchi oshkor bo‘lmagan hodisalarning potensial paydo bo‘lishidir.

№171 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Hujum bu,
Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat.
Ishdan bo‘shab ketgan xodim taqsimlangan diskdan haligacha foydalanish imkoniyatiga ega bo‘lishi mumkinligi.
Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi va ularni uzib qo‘yuvchi oshkor bo‘lmagan hodisalarning potensial paydo bo‘lishidir.
Portlaganida tizim xavfsizligini buzuvchi kutilmagan va oshkor bo‘lmagan hodisalarga olib keluvchi kamchilik, loyihalashdagi yoki amalga oshirishdagi xatolik.

№172 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Tarmoqqa qaratilgan tahdidlar odatda ikki turga ajratiladi:
Ichki va tashqi
Tabiiy va sun’iy
Faol va nofaol
Tizimlashgan va tizimlashmagan

№173 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Tashqi tahdidlar odatda ikki turga ajratiladi:
Tizimlashgan va tizimlashmagan
Ichki va tashqi
Tabiiy va sun’iy
Faol va nofaol

№174 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi. Bu qaysi hujum?

Razvedka hujumlari
Kirish hujumlari
Xizmatdan voz kechishga undash hujumlari
Zararli hujumlar

№175 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Tarmoq haqida axborotni to‘plash hujumchilarga mavjud bo‘lgan potensial zaiflikni aniqlash imkonini beradi. Bu qaysi hujum?
Razvedka hujumlari
Kirish hujumlari
Xizmatdan voz kechishga undash hujumlari
Zararli hujumlar

№176 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. Bu qaysi hujum?
Kirish hujumlari
Xizmatdan voz kechishga undash hujumlari
Zararli hujumlar
Razvedka hujumlari

№177 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Ruxsatsiz foydalanish, qo‘pol kuch hujumi, imtiyozni orttirish, o‘rtaga turgan odam hujumi va hokazolarni o‘z ichiga oladi.
Kirish hujumlari
Xizmatdan voz kechishga undash hujumlari
Zararli hujumlar
Razvedka hujumlari

№178 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

Hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi. Bu qaysi hujum?
Xizmatdan voz kechishga undash hujumlari
Zararli hujumlar
Razvedka hujumlari
Kirish hujumlari

№179 Fan bobi – 4; Bo‘limi – 3; Qiyinlik darajasi – 3;

DOS hujumlari biror axborotni o‘g‘irlanishiga yoki yo‘qolishiga olib kelmasada, biroq tashkilot funksiyasini bajarilmasligiga olib keladi. Bu qaysi hujum?

Xizmatdan voz kechishga undash hujumlari
Zararli hujumlar
Razvedka hujumlari
Kirish hujumlari

№180 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Bu turdagi hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi. Bu qaysi hujum?
Zararli hujumlar
Razvedka hujumlari
Kirish hujumlari
Xizmatdan voz kechishga undash hujumlari

№181 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... programma yoki fayl bo‘lib, komp’yuter tizimiga tahdid qilish imkoniyatiga ega.
Zararli dastur
Zararli hujumlar
Razvedka hujumlari
Kirish hujumlari

№182 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Razvedka hujumlarining turlari?
Aktiv va passiv
Tizimlashgan va tizimlashmagan
Ichki va tashqi
Tabiiy va sun’iy

№183 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... asosan portlarni va operatsion tizimni skanerlashni o‘z ichiga oladi.
Aktiv razvedka hujumlari
Passiv razvedka hujumlari
Tizimlashgan razvedka hujumlari
Tizimlashmagan razvedka hujumlari

№184 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... trafik orqali axborotni to‘plashga harakat qiladi.
Passiv razvedka hujumlari
Tizimlashgan razvedka hujumlari
Tizimlashmagan razvedka hujumlari

Aktiv razvedka hujumlari

№185 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

..... jarayoni TCP/IP tarmog‘ida paketlarni tutib olish, dekodlash, tekshirish va tarjima qilishni o‘z ichiga oladi.
Snifferlash
Ichki snifferlash
Tashqi snifferlash
Simsiz snifferlash

№186 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Tashkilotdagi xodim tashkilot ichidan turib tarmoqni bevosita tutib olishi mumkin. Bu,
Ichki snifferlash
Tashqi snifferlash
Simsiz snifferlash
Snifferlash

№187 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Haker tarmoqni tashqarisidan turib tarmoqlararo ekran darajasida paketlarni tutib olishi va o‘g‘irlashi mumkin. Bu,
Tashqi snifferlash
Simsiz snifferlash
Snifferlash
Ichki snifferlash

№188 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Hujumchi snifferlanuvchi tarmoqning qayerida joylashuvidan qat’iy nazar, simsiz tarmoqlarni keng foydalanilishi natijasida ma’lumotni qo‘lga kiritish imkoniyati mavjud. Bu,
Simsiz snifferlash
Snifferlash
Ichki snifferlash
Tashqi snifferlash

№189 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Tarmoqlararo ekranning asosiy vazifasi:
Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash
Hujumchi snifferlanuvchi tarmoqning qayerida joylashuvidan qat’iy nazar, simsiz tarmoqlarni keng foydalanilishi natijasida ma’lumotni qo‘lga kiritish imkoniyati mavjud.
Haker tarmoqni tashqarisidan turib tarmoqlararo ekran darajasida paketlarni tutib olishi va o‘g‘irlashi mumkin.
Tashkilotdagi xodim tashkilot ichidan turib tarmoqni bevosita tutib olishi mumkin.

№190 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Tarmoqlararo ekranning asosiy vazifasi:
Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo‘lgan murojaatlarini chegaralash
Hujumchi snifferlanuvchi tarmoqning qayerida joylashuvidan qat’iy nazar, simsiz tarmoqlarni keng foydalanilishi natijasida ma’lumotni qo‘lga kiritish imkoniyati mavjud.
Haker tarmoqni tashqarisidan turib tarmoqlararo ekran darajasida paketlarni tutib olishi va o‘g‘irlashi mumkin.
Tashkilotdagi xodim tashkilot ichidan turib tarmoqni bevosita tutib olishi mumkin.

№191 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Asos stansiya deb nomlanib, ikkita istemolchini operatorga ulash uchun xizmat qiladi.
Base Station (BS)
Subscriber Station (SS)
Mobile Station (MS)
Relay Station (RS)

№192 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Ushbu foydalanuvchi stansiyalari asosan ko‘chmas bo‘lgan qurilmalarni o‘z ichiga oladi.
Subscriber Station (SS)
Mobile Station (MS)
Relay Station (RS)
Base Station (BS)

№193 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Ushbu tashkil etuvchilar asosan harakatlanuvchi qurilmalarni o‘z ichiga oladi (mobil telefonlar, noutbuklar).
Mobile Station (MS)
Relay Station (RS)
Base Station (BS)
Subscriber Station (SS)

№194 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Ushbu tashkil etuvchi bir nechta SS stansiyalarni o‘z ichiga oladi.
Relay Station (RS)
Base Station (BS)
Subscriber Station (SS)
Mobile Station (MS)

№195 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
Inson xatosi
G‘arazli hatti harakatlar
Tabiiy sabablar
Tabiiy ofatlar

№196 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
G‘arazli hatti harakatlar
Tabiiy sabablar
Tabiiy ofatlar
Inson xatosi

№197 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi.
Tabiiy sabablar
Tabiiy ofatlar
Inson xatosi
G‘arazli hatti harakatlar

№198 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Tashkilotlar zaxira nusxalash jarayonida inson aralashuvini imkoni boricha kam talab etadigan saqlash vositalarini tanlashi kerak.
Tezlik
Foydalanuvchanlik
Qulaylik
Ishonchlilik

№199 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Tashkilotlar zaxira nusxalash vositalarini har doim foydalanishga yaroqli bo‘lishiga e’tibor qaratishi lozim.
Foydalanuvchanlik
Qulaylik
Ishonchlilik
Tezlik

№200 Fan bobi – 4; Bo‘limi – 3; Qiyinchilik darajasi – 3;

Tashkilot foydalanish uchun oson bo‘lgan zaxira nusxalash vositasini tanlashi shart.
Qulaylik

Ishonchlilik
Tezlik
Foydalanuvchanlik

Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.	Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik
Axborot xavfsizligining asosiy maqsadlaridan biri-bu…	Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish
Konfidentsiallikga to’g’ri ta`rif keltiring.	axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
Yaxlitlikni buzilishi bu - …	Soxtalashtirish va o’zgartirish
... axborotni himoyalash tizimi deyiladi.	Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi
Kompyuter virusi nima?	maxsus yozilgan va zararli dastur
Axborotni himoyalash uchun ... usullari qo’llaniladi.	kodlashtirish, kriptografiya, stegonografiya
Stenografiya mahnosi...	sirli yozuv
Kriptologiya yo’nalishlari nechta?	2
Kriptografiyaning asosiy maqsadi...	maxfiylik, yaxlitlilikni ta`minlash
SMTP - Simple Mail Transfer protokol nima?	elektron pochta protokoli
SKIP protokoli...	Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi
Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar…	uzilish, tutib qolish, o’zgartirish, soxtalashtirish
...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.	konfidentsiallik
Foydalanish huquqini cheklovchi matritsa modeli bu...	Bella La-Padulla modeli
Kommunikatsion qism tizimlarida xavfsizlikni ta`minlanishida necha xil shifrlash ishlatiladi?	2
Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi?	TCP/IP, X.25 protokollar

Himoya tizimi kompleksligiga nimalar orqali erishiladi?	Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali
Kalit – bu …	Matnni shifrlash va shifrini ochish uchun kerakli axborot
Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?	simmetrik kriptotizimlar
Autentifikatsiya nima?	Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi
Identifikatsiya bu- …	Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni
O’rin almashtirish shifri bu - …	Murakkab bo’lmagan kriptografik akslantirish
Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.	2 turga
Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular …	hosil qilish, yig’ish, taqsimlash
Kriptologiya -	axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
Kriptografiyada alifbo –	axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
Simmetrik kriptotizimlarda ... jumlani davom ettiring	shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi
Kriptobardoshlilik deb …	kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
Elektron raqamli imzo deb –	xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
Kriptografiya –	axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
Kriptografiyada matn –	alifbo elementlarining tartiblangan to’plami
Kriptoanaliz –	kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
Shifrlash –	akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi
Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi?	Tez, aniq va maxfiyligiga

Faol hujum turi deb…	Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon
Blokli shifrlash-	shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish
Simmetrik kriptotizmning uzluksiz tizimida …	ochiq matnning har bir harfi va simvoli alohida shifrlanadi
Kripto tizimga qo’yiladigan umumiy talablardan biri	shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak
Quyidagi tengliklardan qaysilari shifrlash va deshifrlashni ifodalaydi?	Ek1(T)=T, Dk2(T1)=T
Berilgan ta`riflardan qaysi biri assimmetrik tizimlarga xos?	Assimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi
Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang	Vijiner matritsasi, Sezar usuli
Akslantirish tushunchasi deb nimaga aytiladi?	1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga
Simmetrik guruh deb nimaga aytiladi?	O’rin almashtirish va joylashtirish
Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?	simmetrik kriptositemalar
Xavfli viruslar bu - …	kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar
Mantiqiy bomba – bu …	Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari
Elektron raqamli imzo tizimi qanday muolajani amalga oshiradi?	raqamli imzoni shakllantirish va tekshirish muolajasi
Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi?	Simmetrik va assimetrik
Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?	Korporativ va umumfoydalanuvchi
Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo’linadi?	Sust va faol
Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?	SMTP, POP yoki IMAR

Axborot resursi – bu?	axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi
Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu?	login
Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu?	parol
Identifikatsiya jarayoni qanday jarayon?	axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
Autentifikatsiya jarayoni qanday jarayon?	ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
Avtorizatsiya jarayoni qanday jarayon?	foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
Ro’yxatdan o’tish bu?	foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
Axborot qanday sifatlarga ega bo’lishi kerak?	ishonchli, qimmatli va to’liq
Axborotning eng kichik o’lchov birligi nima?	bit
Elektronhujjatning rekvizitlari nechta qismdan iborat?	4
Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?	fleshka, CD va DVD disklar
Imzo bu nima ?	hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati.
Muhr bu nima?	hujjatning haqi-qiyligini va biror bir yuridik shaxsga tegishli ekanligi-ni tasdiqlovchi isbotdir.
DSA – nima	Raqamli imzo algoritmi
El Gamal algoritmi qanday algoritm	Shifrlash algoritmi va raqamli imzo algoritmi
Sezarning shifrlash sistemasining kamchiligi	Harflarning so’zlarda kelish chastotasini yashirmaydi

Axborot xavfsizligi va xavfsizlik san’ati haqidagi fan …. deyiladi?	Kriptografiya
Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu -	steganografiya
Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?	Deshifrlash
…… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.	Kiberxavfsizlik
Risk	Potensial foyda yoki zarar
Kiberxavfsizlik nechta bilim soxasini o‘z ichiga oladi.	8
“Ma’lumotlar xavfsizligi” bilim sohasi.....	ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.
“Dasturiy ta’minotlar xavfsizligi” bilim sohasi.....	foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.
“Tashkil etuvchilar xavfsizligi”	katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.
“Aloqa xavfsizligi” bilim sohasi.....	tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.
“Tizim xavfsizligi” bilim sohasi……	tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi.
“Inson xavfsizligi” bilim sohasi….	kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.
“Tashkilot xavfsizligi” bilim sohasi ….	tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini

“Jamoat xavfsizligi” bilim sohasi …..	u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi.
Tahdid nima? tizim yoki	Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.
Kodlash nima?	Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir
Shifrlash nima?	Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi
Bir martalik bloknotda Qanday kalitlardan foydalaniladi?	Ochiq kalitdan
Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing.	23
Agar RSA algotirmida n ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.	$M = C^d \bmod n$;
O’nlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq tizi miga o’tkazing. 65	100001
Quyidagi modulli ifodani qiymatini toping. (125*45)mod10.	5
Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256.	244
Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.	$C = M^e \bmod n$; -tog’ri javob
Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi	Kriptologiya.
Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi	$\{d, n\}$ – yopiq, $\{e, n\}$ – ochiq;
Zamonaviy kriptografiya qanday bo’limlardan iborat?	Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish
1. Kriptografik usullardan foydalanishning asosiy yo’nalishlari nimalardan iborat?	Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarni haqiqiyligini aniqlash, tashuvchilarda axborotlarni shifrlangan ko’rinishda saqlash (masalan, hujjatlarni, ma’lumotlar bazasini)

Shifr nima?	Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm
Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?	Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi
Oqimli shifrlashning mohiyati nimada?	Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur, Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi
Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating.	uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim,
Kriptotizim quyidagi komponentlardan iborat:	ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, Ek : M $\rightarrow$ C (shifrlash uchun) va Dk: C$\rightarrow$M (deshifrlash uchun) funktsiyalar
Serpent, Square, Twofish, RC6 , AES algoritmlari qaysi turiga mansub?	simmetrik blokli algoritmlar
DES algoritmiga muqobil bo’lgan algoritmni ko’rsating.	Uch karrali DES, IDEA, Rijndael
DES algoritmining asosiy muammosi nimada?	kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas
Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?	shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun
12+22 mod 32 ?	2
2+5 mod32 ?	7

Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi.	ochiq kalitlar
12+11 mod 16 ?	7
RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo’llab quvvatlaydi.	128 bitli, 192 bitli, 256 bitli
Xesh-funktsiyani natijasi …	uzunlikdagi xabar
RSA algoritmi qanday jarayonlardan tashkil topgan	Kalitni generatsiyalash; Shifrlash; Deshifrlash.
RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida necha bit bo‘lishi talab etiladi.	2048
Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi	Xesh funksiyalar
To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub	Xalqa
Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo’llamasligi mumkin	to’liq bog’lanishli
Kompyuterning tashqi interfeysi deganda nima tushuniladi	kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari
Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi	Yulduz
Ethernet kontsentratori qanday vazifani bajaradi	kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi
OSI modelida nechta sath mavjud	7
OSI modelining to’rtinchi sathi qanday nomlanadi	Transport sathi
OSI modelining beshinchi sathi qanday nomlanadi	Seanslar sathi
OSI modelining birinchi sathi qanday nomlanadi	Fizik sath
OSI modelining ikkinchi sathi qanday nomlanadi	Kanal sathi
OSI modelining uchinchi sathi qanday nomlanadi	Tarmoq sathi
OSI modelining oltinchi sathi qanday nomlanadi	Taqdimlash sathi
OSI modelining ettinchi sathi qanday nomlanadi	Amaliy sath
OSI modelining qaysi sathlari tarmoqqa bog’liq sathlar hisoblanadi	fizik, kanal va tarmoq sathlari
OSI modelining tarmoq sathi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi	Marshrutizator
Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi	Fizik sath
Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi sathi bajaradi	Tarmoq sathi
Keltirilgan protokollarning qaysilari tarmoq sathi protokollariga mansub	IP, IPX
Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub	TCP,UDP

OSI modelining fizik sathi qanday funktsiyalarni bajaradi	Elektr signallarini uzatish va qabul qilish
OSI modeliningamaliy sathi qanday funktsiyalarni bajaradi	Klient dasturlari bilan o’zaro muloqotda bo’lish
Keltirilgan protokollarning qaysilari kanal sathi protokollariga mansub	Ethernet, FDDI
Keltirilgan protokollarning qaysilari taqdimlash sathi protokollariga mansub	SNMP, Telnet
Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...	Avtorizatsiya
Autentifikatsiya faktorlari nechta	3
Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima	Parol
Ko‘z pardasi, yuz tuzilishi, ovoz tembri.	Biometrik autentifikatsiya
barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi.	Fizik satx
Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi	2
Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi.	Foydalanishni boshqarish
Foydalanishni boshqarish –bu...	sub’ektni sub’ektga ishlash qobilyatini aniqlashdir.
Foydalanishna boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi,	Sub’ekt
Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ?	Ob’ekt
Foydalanishna boshqarishning nechta usuli mavjud?	4
Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy ob’ektlarni himoyalash uchun qo‘llaniladi	DAC
Foydalanishni boshqarishning qaysi modelida ob’ekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi	DAC
Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi.	MAC
Foydalanishni boshqarishning mandatli modelida Ob’ektning xavfsizlik darajasi nimaga bog‘liq..	Tashkilotda ob’ektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi
MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi	xavfsizlik siyosati ma’muri

Agar sub’ektning xavfsizlik darajasida ob’ektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi	O‘qish
Agar sub’ektning xavfsizlik darajasi ob’ektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.	Yozish
Foydalanishni boshqarishning qaysi modelida har bir ob’ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun ob’ektlardan foydalanish ruxsati ko‘rsatiladi?	RBAC
Rol tushunchasiga ta’rif bering.	Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin
Foydalanishni boshqarishning qaysi usuli - ob’ektlar va sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.	ABAC
XACML foydalanishni boshqarishni qaysi usulining standarti?	ABAC
Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?	barchasi
Axborotning kriptografik himoya vositalari necha turda?	3
Dasturiy shifrlash vositalari necha turga bo‘linadi	4
Diskni shifrlash nima uchun amalga oshiriladi?	Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?	4
Kompyuter tarmoqlari bu –	Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi
Tarmoq modeli –bu.. ikki	Hisoblash tizimlariorasidagi aloqani ularning ichki tuzilmaviy vatexnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir to‘plami
OSI modelida nechta tarmoq sathi bor	7
OSI modeli 7 stahi bu	Ilova
OSI modeli 1 stahi bu	Fizik
OSI modeli 2 stahi bu	Kanal
TCP/IP modelida nechta satx mavjud	4

Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi.	Shaxsiy tarmoq
Tarmoq kartasi bu...	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
Switch bu...	Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
Hab bu...	ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
Tarmoq repiteri bu...	Signalni tiklash yoki qaytarish uchun foydalaniladi.
Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi.	DNS tizimlari
….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.	TCP
…. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.	UDP
Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi.	IP
Tarmoq taxdidlari necha turga bo‘linadi	4
Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;	Razvedka hujumlari
Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi	Kirish hujumlari
Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;	Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;	Zararli hujumlar
Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?	Imzo qo‘yish va imzoni tekshirishdan
Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi?	Imzo muallifining ochiq *kaliti yordamida*
Tarmoq modeli-bu...	Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir
OSI modeli nechta sathga ajraladi?	7

Fizik sathning vazifasi nimadan iborat	Qurilma, signal va binar o‘zgartirishlar
Ilova sathning vazifasi nimadan iborat	Ilovalarni tarmoqqa ulanish jarayoni
Kanal sathning vazifasi nimadan iborat	Fizik manzillash
Tarmoq sathning vazifasi nimadan iborat	Yo‘lni aniqlash va mantiqiy manzillash
TCP/IP modeli nechta sathdan iborat	4
Quyidagilarninf qaysi biri Kanal sathi protokollari	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35.
Quyidagilarninf qaysi biri tarmoq sathi protokollari	. IP, ICMP, ARP, RARP
Quyidagilarninf qaysi biri transport sathi protokollari	TCP, UDP, RTP
Quyidagilarninf qaysi biri ilova sathi protokollari	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP va hak
TCP/IP modelining kanal sathiga OSI modelining qaysi sathlari mos keladi	Kanal, Fizik
TCP/IP modelining tarmoq sathiga OSI modelining qaysi sathlari mos keladi	Tarmoq
TCP/IP modelining transport sathiga OSI modelining qaysi sathlari mos keladi	Tramsport
TCP/IP modelining ilova sathiga OSI modelining qaysi sathlari mos keladi	Ilova, taqdimot, seans
Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.	Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.	. Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang.	Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi
Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang.	Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi
Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan	Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi
Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan	Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi
Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan	Yuboriluvchi va qabul qilinuvchi ma’lumot TOKYeN yordamida manziliga yetkaziladi

Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan	Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi
Tarmoq kartasi nima?	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
Repetir nima?	Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
Hub nima?	Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
Switch nima?	Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
Router nima?	Qabul qilingan ma’lumotlarni tarmoq sathiga tegishli manzillarga ko‘ra (IP manzil) uzatadi
DNS tizimlari.	Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi
TCP bu- …	Transmission Control Protocol
UDP bu-…	User datagram protocol
Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang	Ichki, tashqi
Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi	Biznes jarayonlarni to‘xtab qolishiga olib keladi
Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi	Hujum natijasida ishlab chiqarishi yo‘qolgan hollarda uni qayta tiklash ko‘p vaqt talab qiladi va bu vaqtda ishlab chiqarish to‘xtab qoladi
Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi	Konfidensial axborotni chiqib ketishi natijasida, tashkilot shaxsiy ma’lumotlarini yo‘qolishi mumkin
Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi	Tashkilot xodimlarining shaxsiy va ishga oid ma’ulmotlarini kutilmaganda oshkor bo‘lishi ushbu xodimlarga bevosita ta’sir qiladi

Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi	Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi
Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi	tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi
Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi.	Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.
Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi	Razvedka hujumlari
Ma’lumotlarni zaxira nusxalash bu – …	Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi
Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz	Zaxira nusxalash
Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering	Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi?	5
Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi.	4
Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash	Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart.
RAID texnologiyasining transkripsiyasi qanday.	Random Array of Independent Disks
RAID texnologiyasida nechta satx mavjud	6
OSI modelining birinchi sathi qanday nomlanadi	Fizik sath
OSI modelining ikkinchi sathi qanday nomlanadi	Kanal sathi
OSI modelining uchinchi sathi qanday nomlanadi	Tarmoq sathi
OSI modelining oltinchi sathi qanday nomlanadi	Taqdimlash sathi
OSI modelining ettinchi sathi qanday nomlanadi	Amaliy sath

Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi	Fizik sath
Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub	TCP,UDP
OSI modelining fizik sathi qanday funktsiyalarni bajaradi	Elektr signallarini uzatish va qabul qilish
OSI modelining amaliy sathi qanday funktsiyalarni bajaradi	Klient dasturlari bilan o’zaro muloqotda bo’lish
12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan sonlar soni nechta?	8 ta
Yevklid algoritmi qanday natijani beradi?	Sonning eng katta umumiy bo’luvchisini toppish
Qanday sonlar tub sonlar deb yuritiladi?	Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi.
To‘liq zaxiralash	To‘liq va o‘sib boruvchi usullarning mujassamlashgan ko‘rinishi bo‘lib, oxirgi zaxiralangan nusxadan boshlab bo‘lgan o‘zgarishlarni zaxira nusxalab boradi. • Amalga oshirish to‘liq zaxiralashga qaraganda tez amalga oshiriladi. • Qayta tiklash o‘sib boruvchi zaxiralashga qaraganda tez amalga oshiriladi. • Ma’lumotni saqlash uchun to‘liq zaxiralashga qaraganda kam joy talab etadi

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

Fire Wall ning vazifasi...	tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi
Kompyuter virusi nima?	maxsus yozilgan va zararli dastur
Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating	disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali
Troyan dasturlari bu...	virus dasturlar
Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi?	5
Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud	detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar
Axborotni himoyalash uchun ... usullari qo’llaniladi.	kodlashtirish, kriptografiya, stegonografiya
Stenografiya mahnosi...	sirli yozuv
…sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi	K.Shennon
Kriptologiya yo’nalishlari nechta?	2
Kriptografiyaning asosiy maqsadi...	maxfiylik, yaxlitlilikni ta`minlash
Zararli dasturiy vositalarni aniqlash turlari nechta	3
Signaiurana asoslangan	...bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin.
O‘zgarishni aniqlashga asoslangan	Zararli dasturlar biror joyda joylashishi sababli, agar tizimdagi biror joyga o‘zgarishni aniqlansa, u holda u zararlanishni ko‘rsatishi mumkin
Anomaliyaga asoslangan	Noodatiy yoki virusga o‘xshash yoki potensial zararli harakatlari yoki xususiyatlarni topishni maqsad qiladi
Antiairuslar qanday usulda viruslarni aniqlaydi	Signaturaga asoslangan
Viruslar -	o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi
Rootkitlar-	ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi

Backdoorlar -	zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish
Troyan otlari-	bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi
Ransomware-	mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi
Resurslardan foydalanish usuliga ko’ra viruslar qanday turlarga bo’linadi	Virus parazit, Virus cherv
Zararlagan obyektlar turiga ko’ra	Dasturiy, yuklanuvchi, Makroviruslar, multiplatformali viruslar
Faollashish prinspiga ko’ra	Resident, Norezident
Dastur kodini tashkil qilish yondashuviga ko‘ra	Shifrlangan, shifrlanmagan, Polimorf
Shifrlanmagan viruslar	o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi.
P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang	840
256mod25=?	6
bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi.	Tizim
Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima duyidadi	Xavfsizlik siyosati
RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday?	p va q –sonlarning ko‘paytmasini ifodalovchi sonning spektoriga teng;
DES algoritmi akslantirishlari raundlari soni qancha?	16;
DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha?	CHap qism blok 32 bit, o‘ng qism blok 32 bit;
Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor?	SHifrlash va deshifrlash jarayonlari uchun kalitlarni generatsiya qilish qoidalariga ko‘ra farqlanadi
19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta?	18 ta

10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta?	4 ta
Eyler funsiyasida $\phi(1)$ qiymati nimaga teng?	0
Eyler funksiyasida 60 sonining qiymatini toping.	59
Eyler funksiyasi yordamida 1811 sonining qiymatini toping.	1810
97 tub sonmi?	Tub
Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256.	244
Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220	44
Quyidagi ifodani qiymatini toping. -17mod11	5
2 soniga 10 modul bo’yicha teskari sonni toping.	Ø
Tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta’minlash sohasidagi tadbirlar tavsiflanadigan yuqori darajadagi reja nima?	Kiberxavfsizlik siyosati
Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi?	tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi
Kiberxavfsizlikni ta’minlash masalalari bo’yicha xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang	SANS (System Administration Networking and Security)
Korxonaning davomli muvaffaqiyat bilan faoliyat yuritishini ta’minlashga mo’ljallangan strukturalangan va o’zaro bog’langan harakatlar to’plami- …	Strategiya
Tahdidlarning muvaffaqiyatli amalga oshirilishiga imkon beruvchi har qanday omil – bu …	Zaiflik
ISO/IEC 27002:2005 – ….	Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari
O’zDStISO/IEC 27005:2013 – ….	Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish
Axborot xavfsizligi arxitekturasining nechta satxi bor?	3
Rahbariy hujjat. Ma’lumotlar uzatish tarmog’ida axborot xavfsizligini ta’minlash to’g’risida Nizom - Xujjat raqamini toping	RH 45-215:2009
Davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta’minlash dasturini ishlab chiqish tartibi - Xujjat raqamini toping	RH 45-185:2011

Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta’minlash darajasini aniqlash tartibi - Xujjat raqamini toping	RH 45-193:2007
Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta’riflar - Xujjat raqamini toping	TSt 45-010:2010
Quyidagilardan qaysi standart aloqa va axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta’riflarni belgilaydi?	TSt 45-010:2010
Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni nima?	Identifikatsiya
Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima?	Autentifikatsiya
Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni – nima deyiladi?	Avtorizatsiya
Identifikatsiya nima?	Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni
Autentifikatsiya nima?	Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni
Avtorizatsiya nima?	Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni
... - Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o’tishni ta’minlovchi biror axborot	Parol
Smart karta o’lchamidagi, kichik xajmdagi xotira va xisoblash imkoniyatiga ega bo’lgan, o’zida parol yoki kalitni saqlovchi qurilma nima deb ataladi?	Token, Smartkarta
Smarkarta nima asosida autentifikatsiyalaydi?	Something you have
Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o’zgarib turadigan parol nima deyiladi?	One-time password (OTP)

Foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish nima deb ataladi?	Ma’murlash
Amaldagi qonunchilikka mos ravishda texnik, dasturiy va dasturiy-texnik vositalar yordamida axborot xavfsizligining nokriptografik usullari bilan ta’minlashni inobatga oluvchi axborot himoyasi nima?	Axborotning texnik himoyasi
Nazorat hududi – bu ...	Qo’riqlanuvchi soha bo’lib, uning ichida kommunikatsiya qurilmalari hamda axborot tarmog’ining lokal tarkibiy qurilmalarini birlashtiruvchi barcha nuqtalar joylashadi
Texnik himoya vositalari – bu ...	Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob’ektni himoyalashdir
Bu axborotni tutib olish qurilmasi bo’lib, ularda uzatuvchi qurilma sifatida kontaktli mikrofonlardan foydalaniladi	Stetoskoplar
Xesh funktsiya to’g’ri ko’rsatilgan javobni aniqlang.	MD5
MD5, SHA1, Tiger xesh funktsiyalari uchun blok uzunligi necha baytga teng?	64 bayt
Sub’ektni ob’ektga ishlash qobilyatini aniqlash – nima?	Foydalanishni boshqarish
Foydalanishni boshqarishda sub’ekt bu -	Inson, dastur, jarayon
Foydalanishni boshqarishning qaysi usuli tizimdagi shaxsiy ob’ektlarni ximoyalash uchun qo’llaniladi?	Discretionary access control DAC
Foydalanishni boshqarishning qaysi usulidan asosan operatsion tizimlarda qo’llaniladi?	Discretionary access control DAC
Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi?	Mandatory access control MAC
Foydalanishni boshqarishning qaysi usulida xavfsizlik markazlashgan tarzda xavfsizlik siyosati m’muri tomonidan amalga oshiriladi?	Mandatory access control MAC
Foydalanishni boshqarishning qaysi usulida xar bir foydalanuvchini foydalanish ruxsatini belgilash o’rniga rol uchun ob’ektlardan foydalanish ruxsatini ko’rsatish yetarli bo’ladi?	Role-based access control RBAC
Foydalanishni boshqarishning qaysi usulida sub’ekt va ob’ektlarga tegishli xuquqlarni ma’murlash oson kechadi?	Role-based access control RBAC

Firibgarlikni oldini olish uchun bir shaxs tomonidan ko’plab vazifalarni bajarishga ruxsat bermaslik zarur. Bu muammo foydalanishni boshqarishni qaysi usulida bartaraf etiladi?	Role-based access control RBAC
Ob’ekt va sub’ektlarning attributlari, ular bilan mumkin bo’lgan amallar va so’rovlarga mos keladigan muxit uchun qoidalarni taxlil qilish asosida foydalanishni boshqarish -	Attribute based access control ABAC
Attribute based access control ABAC usuli attributlari qaysilar?	Foydalanuvchi attributlari, Resurs attributlari, Ob’ekt va muxit attributlari
Foydalanishni boshqarishning qaysi usulida ruxsatlar va xarakatni kim bajarayotganligi to’g’risidagi xolatlar “agar, u xolda” buyrug’idan tashkil topgan qoidalarga asoslanadi?	Attribute based access control ABAC
XASML standarti foydalanishni boshqarishning qaysi usulida qo’llaniladi?	Attribute based access control ABAC
XASML standartida qoida nima?	Maqsad, ta’sir, shart, majburiyat va maslaxatlar
XASML standartida maqsad nima?	Sub’ekt ob’ekt ustida nima xarakat qilishi
Lampsonning foydalanishni boshqarish matritsasi nimalardan tashkil topgan?	Imtiyozlar ro’yxati
Access control list va Capability list bu nimaning asosiy elementi xisoblanadi?	Lampson matritsasining
Lampson matritsasining satrlarida nima ifodalanadi?	Sub’ektlar
Foydalanishni boshqarishning mantiqiy vositalari infratuzilma va uning ichidagi tizimlarda ... uchun foydalaniladi.	Mandat, Tasdiqlash, Avtorizatsiya
SHaxsiy simsiz tarmoq standartini aniqlang.	Bluetooth, IEEE 802.15, IRDA
Lokal simsiz tarmoq standartini aniqlang.	IEEE 802.11, Wi-Fi, HiperLAN
Regional simsiz tarmoq standartini aniqlang.	IEEE 802.16, WiMAX
Global simsiz tarmoq standartini aniqlang.	CDPD, 2G, 2.5G, 3G, 4G, 5G
Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang.	SHaxsiy simsiz tarmoq
IEEE 802.11, Wi-Fi, HiperLAN standartida ishlovchi simsiz tarmoq turini aniqlang.	Lokal simsiz tarmoq
IEEE 802.16, WiMAX standartida ishlovchi simsiz tarmoq turini aniqlang.	Regional simsiz tarmoq
CDPD, 2G, 2.5G, 3G, 4G, 5G standartida ishlovchi simsiz tarmoq turini aniqlang.	Global simsiz tarmoq
Bluetooth qanday chastota oralig’ida ishlaydi?	2.4-2.485 Ggts
Wi-Fi qanday chastota oralig’ida ishlaydi?	2.4-5 Ggts
WiMax tarmog’ining tezligi qancha?	1 Gbit/sekund
Quyidagilardan qaysi biri MITM xujumiga tegishli xatti-xarakat ximoblanadi?	Aloqa seansini konfidentsialligini va yaxlitligini buzish

WiMAX tarmoq arxitekturasi nechta tashkil etuvchidan iborat?	5
WiMAX tarmoq arxitekturasi qaysi tashkil etuvchidan iborat?	Base station, Subscriber station, Mobile station, Relay station, Operator network
GSM raqamli mobil telefonlarining nechanchi avlodi uchun ishlab chiqilgan protokol?	Ikkinchi avlodi
GSM standarti qaysi tashkilot tomonidan ishlab chiqilgan?	European telecommunications standards institute
.... – o'zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma'lumoti va xavfsizlik algoritmlarini saqlaydi.	Sim karta
Rutoken S qurilmasining og'irligi qancha?	6.3 gramm
True Crypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?	AES, Serpent, Twofish
Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidentsialligini aniqlash qaysi dasturiy shifrlash vositalarining vazifasi?	Disc encryption software
BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?	AES, Serpent, Twofish
AxCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?	AES-256
Qog'oz ko'rinishidagi axborotlarni yo'q qilish qurilmasining nomini kiriting.	Shreder
Ma'lumotlarni bloklarga bo'lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?	RAID 0
Qaysi texnologiyada ma'lumotni ko'plab nusxalari bir vaqtda bir necha disklarga yoziladi?	RAID 1
Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi?	RAID 3
Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?	RAID 5
Disk zararlanganda "qaynoq almashtirish" yordamida uni almashtirish mumkin. Bu xususiyat qaysi texnologiyaga tegishli?	RAID 50
Zaxiralashning qanday turlari mavjud?	To'liq, o'sib boruvchi, differentsial
IOS, Android, USB xotiralardan ma'lumotlarni tiklash uchun qaysi dasturdan foydalaniladi?	EASEUS Data recovery wizard
Foydalanuvchi ma'lumotlarini qo'lga kirituvchi va uni xujumchiga yuboruvchi dasturiy kod nima?	Spyware
Operatsion tizim tomonidan aniqlanmasligi uchun ma'lum xarakatlarni yashirish nima deyiladi?	Rootkits
Qurbon kompyuterda mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo'yib to'lov amalga oshirishni talab qiladi. Bu qaysi zararli dastur?	Ransomware
Quyidagilardan o'zidan ko'payishi yo'q bo'lganlarini belgilang.	Mantiqiy bomba, Troyan oti, Backdoors

Viruslar resurslardan foydalanish usuliga ko’ra qanday turlarga bo’linadi?	Virus parazitlar, virus chervlar
Viruslar zararlangan ob’ektlar turiga ko’ra qanday turlarga bo’linadi?	Dasturiy, yuklanuvchi, makroviruslar, ko’p platformali
Viruslar faollashish printsipiga ko’ra qanday turlarga bo’linadi?	Rezident, norezident
Viruslar dastur kodini tashkil qilish yondoshuviga ko’ra qanday turlarga bo’linadi?	SHifrlangan, shifrlanmagan, polimorf
Dastlabki virus nechanchi yilda yaratilgan?	1988
ILOVEYOU virusi keltirgan zarar qancha?	10 mlrd. Dollar
CodeRed virusi keltirgan zarar qancha?	2 mlrd. Dollar
Melissa virusi keltirgan zarar qancha?	80 million dollar
NetSky virusi keltirgan zarar qancha?	18 mlrd. Dollar
MyDoom virusi keltirgan zarar qancha?	38 mlrd. Dollar
Risk monitoring ….. ni paydo bo’lish imkoniyatini aniqlaydi.	Yangi risklar
….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.	Risk monitoring
Axborot xavfsizligi siyoatining necha hil turi bor?	3
Internetdan foydalanish siyosatining nechta turi mavjud?	4
Nomuntazam siyosat (Promiscuous Policy) nima?	Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi
Paranoid siyosati (Paranoid Policy) – bu ….	Hamma narsa ta’qiqlanadi
Ruxsat berishga asoslangan siyosat (Permissive Policy) – bu …	Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi
Ehtiyotkorlik siyosati (Prudent Policy) – bu ….	Barcha hizmatlar blokirovka qilingandan so’ng bog’lanadi
Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi. Bu qaysi xavfsizlik siyosatiga hos?	Nomuntazam siyosat (Promiscuous Policy)
Barcha hizmatlar blokirovka qilingandan so’ng bog’lanadi. Bu qaysi xavfsizlik siyosatiga hos?	Ehtiyotkorlik siyosati (Prudent Policy)
Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi. Bu qaysi xavfsizlik siyosatiga hos?	Ruxsat berishga asoslangan siyosat (Permissive Policy)
Hamma narsa ta’qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?	Paranoid siyosati (Paranoid Policy)
Tizim arxitekturasining turlari nechta?	5
Internet, havo hujumidan mudofaa, transport tizimlari qaysi tizim arxitekturasiga xos?	Hamkorlik tizimlari arxitekturasi
Cloud computing texnologiyasining nechta asosiy turi mavjud?	3
Raqamli soatlar qaysi texnologiyaga tegishli?	O’rnatilgan tizimlar (Embedde systems)

```
?
1.Axborot xavfsizligini taíminlaydigan nechta asosiy tamoyili mavjud?
+3 ta
-2 ta
```

-4 ta
-5 ta

?
2.´To'q sariq kitobªning birinchi qismi nimaga bagíishlangan?
+Izohning o'ziga bagíishlangan
-Kirishga bagíishlangan
-Xavfsizlikga bagíishlangan
-Chora tadbirlarga bagíishlangan

?
3.´To'q sariq kitobªning ikkinchi qismi nimaga bagíishlangan?
+tarmoq konfiguratsiyalari uchun muhim bo'lgan xavfsizlik servislari tavsiflangan
-Izohning o'ziga bagíishlangan uchun muhim bo'lgan xavfsizlik ko'nikmalari tavsiflangan holda
-Kirishga bagíishlangan
-Chora tadbirlarga bagíishlangan
?
4.Adaptiv xavfsizlikda korporativ tarmoqdagi shubhali harakatlarni baholash jarayoniñbu:
+Hujumlarni aniqlash
-Himoyalashni tahlillash
-Xavf -xatarni baholash
-Zaifliklarni aniqlash
?
5.Adaptiv xavfsizlikda tarmoqning zaif joylarini qidirish qaysi jarayon orqali bajariladi?
+Himoyalashni tahlillash
-Xavf -xatarni baholash
-Hujumlarni aniqlash
-Bardoshlilikni hisoblash
?
6.Adaptiv xavfsizlikda zaifliklarni (keltiradigan zararning jiddiylik darajasi boëyicha), tarmoq qism tizimlarini (jiddiylik darajasi boëyicha), tahdidlarni aniqlash va rutbalashga nima imkon beradi?
+Xavf-xatarni baholash
-Himoyalashni tahlillash
-Hujumlarni aniqlash
-Bardoshlilikni hisoblash
?
7.Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishi bilan bog'liq bo'lsa bu nima deb yuritiladi?
+Jinoyat sifatida baholanadi
-Ragíbat hisoblanadi
-Buzgunchilik hisoblanadi
-Guruhlar kurashi hisoblanadi
?
8.Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taíminlashning zaruriy shartiñbu:
+Tamoqlararo ekranlarning oërnatilishi
-Tashkiliy ishlarni bajarilishi
-Globol tarmoqdan uzib qoëyish
-Aloka kanallarida optik toladan foydalanish
?
9.Aloqa kanallarida maílumotlarni himoyalash masalasini echish usullarini nechta guruhi mavjud?
+3ta
-2ta
-4ta
-5ta
?
10.AlÓqa kanallarida ma`lumÓtlarni uzatishni himÓyalash vazifalariga nimalar kiradi?
+Xabarlar mazmunining fÓsh qilinishini va xabarlar Óqimining tahlillanishini Óldini Ólish
-Ma`lumÓtlarni uzatuvchi tarmÓqning buzilganligini aniqlash va ularni qiyosiy taxlillarini kuzatib boradi
-Tizim nazoratini buzilganligini aniqlash
-Shifrlash kalitlarini buzilganligini aniqlash
?
11.AQShning axborotni shifrlash standartini keltirilgan javobni koírsating?
+DES(Data Encryption Standart)
-RSA (Rivest, Shamir ,‡ Adleman)
-AES (Advanced Encryption Standart)
-Aniq standart ishlatilmaydi

?
12.Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun qanday axborot ishlatiladi?
+Ikkita kalit
-Bitta kalit
-Elektron raqamli imzo
-Foydalanuvchi identifikatori
?
13.Autentifikatsiya prÓtÓkÓllariga boíladigan asÓsiy hujumlarni koírsating?
+Autentifikatsiya almashinuvining taraflarini almashtirib qoíyish, majburian kechikish, matn tanlashli hujumlar
-Xizmat koírsatishdan vÓz kechish hujumlari
-KÓmp yuter tizimini ishdan chiqaruvchi hujumlar va autentifikatsiya jaroyonlariga halaqit berish uchun hujum qilinadi
-DOS va DDOS hujumlar
?
14.Avtorizatsiya tizimdan foydalanishda qanday vakolat berani?
+Sub'ektning harakat doirasi va foydalanadigan resurslarni belgilaydi
-Resurslardan foydalanishga imkon beradi va obyekni to'g'ri ishlashini nazorat beradi
-Resurslarni oízgartirishga imkon beradi
-Sub'ektni foydalanishi taqiqlangan resurslarni belgilaydi
?
15.Axborot xavfsizligi strategiyasi va himoya tizimi arxitekturasi nima asosida ishlab chiqiladi?
+Axborot xavfsizligi konsepsiyasi
-Standartlar va halqoro standartlar markazi
-Farmonlar
-Buyruqlar
?
16.Axborot himoyasini umumiy strategiyasining muhim xususiyati-bu:
+Xavfsizlik tizimini tadqiqlash
-Tizim obíektlarini aniqlash
-Tizimni boshqarishni optimallashtirish
-Tizimni skanerlash jarayoni
?
17.Axborot paketlarini qachon ushlab qolish mumkin?
+Aloqa kanallari orqali uzatishda
-Xotira qurilmalarida saqlanayotganda
-Kompyuter ishgan tushganda
-Maílumotlar nusxalanayotganda
?
18.Axborot quroli-bu:
+Axborot massivlarini yoëqotish, buzish yoki oëgëirlash vositalari, himoyalash tizimini yoëqotish vositalari
-Axborot makoni yaratish, oëzgartirish yoki tezlashtirish vositalari
-Kuzatish yoki oëgëirlash vositalarini yaratish, himoyalash tizimini qoëllab quvvatlash vositalarini tahlil qilish jarayoni
-Axborot tashuvchilar yoki nusxalash vositalari, himoyalash tizimini kuchaytirish vositalari
?
19Axborot tizimini samarali himoyasini loyihalash va amalga oshirish bosqichlari qaysi javobda to'g'ri ko'rsatilgan.
+Xavf-xatarni tahlillash, xavfsizlik siyosatini amalga oshirish, xavfsizlik siyosatini madadlash
-Himoya obíektlarini aniqlash, hujumlarni tahlillash
-Tarmoq va foydalanuvchilarni nazoratlash, tarmoq himoyasini qurish
-Xavf-xatarlarni baholash, loyihalash boíyicha choralar ishlab chiqish va jarayonni urganishni ta'minlash yullari
?
20.Axborot xavfsizligi konsepsiyani ishlab chiqish necha bosqichni oëz ichiga oladi?
+3 bosqichni
-4 bosqichni
-5 bosqichni
-6 bosqichni
?
21.Axborot xavfsizligi siyosatida ishlashning muayyan qoidalari nimalarni belgilaydi?
+Nima ruxsat etilishini va nima ruxsat etilmasligini
-Axborotni himoyalash vositalarini toëplamlari
-Xavfsizlikni amalga oshirish vaqti me¸yorlari
-Axborotni himoyalash bosqichlari
?
22.Axborot xavfsizligi siyosatini ishlab chiqishda avvalo nimalar aniqlanadi?

+Himoya qilinuvchi obíekt va uning vazifalari
-Mavjud himoya vositalari
-Himoya tizimiga talablar
-Himoya tizimini tashkil etish muddati va vazifasi
?
23.Axborot xavfsizligi siyosatining umumiy prinsplari nimani aniqlaydi?
+Internetda xavfsizlikga yondashuvi
-Axborot himoyalash vositalarini toëplamlari
-Xavfsizlikni amalga oshirish vaqti meíyorlari
-Axborotni himoyalash bosqichlari
?
24.Axborot xavfsizligi strategiyasi va himoya tizimi arxitekturasi nima asosida ishlab chiqiladi?
+Axborot xavfsizligi konsepsiyasi asosida
-Tizimni loyihalashda yuzaga keladigan vaziyat asosida
-Axborot tizimi qurilmalarini soddalashtirish asosida
-Himoyani buzishga boílgan urinishlar asosida
?
25.Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?
+Axborot xavfsizligi buzulgan taqdirda koírilishi mumkin boílgan zarar miqdori bilan
-Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhumligi bilan
-Axborotni noqonuniy foydalanishlardan oízgartirishlardan va yoíq qilishlardan himoyalanganligi bilan
-Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bilan
?
26.Axborot xavfsizligida nima boëyicha ikkinchi oërinni oëgëirlashlar va soxtalashtirishlar egallaydi?
+Zarar ulchami boëyicha
-Axborot muximligi boëyicha
-Axborot xajmi boëyicha
-Foyda xajmi boëyicha
?
27.Axborot xavfsizligiga boëladigan ma¸lum taxdidlardan ximoyalash mexanizmini maílumotlarni uzatish tarmogëi arxitekturasiga qay tarzda joriy etilishi lozimligini belgilaydi-bu:
+Arxitekturaviy talablar
-Texnik talablar
-Boshqarish (ma¸muriy talablar)
-Funksional talablar
?
28.Axborot xavfsizligiga boëladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?
+Strukturalarni ruxsatsiz modifikatsiyalash
-Tabiy ofat va avariya
-Texnik vositalarning buzilishi va ishlamasligi
-Foydalanuvchilar va xizmat koërsatuvchi hodimlarning hatoliklari
?
29.Axborot xavfsizligiga boëladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?
+Texnik vositalarning buzilishi va ishlamasligi
-Axborotdan ruhsatsiz foydalanish
-Zararkunanda dasturlar
-Aníanaviy josuslik va diversiya haqidagi ma'lumotlar tahlili
?
30.Axborot xavfsizligini buzuvchilarni qanday kategoriyalarga ajratish mumkin?
+1- sarguzasht qidiruvchilar,2- gíoyaviy xakerlar, 3- xakerlar-professionallar, 4- ishonchsiz xodimlar
-1- buzgunchilar, 2- gíoyaviy xakerlar, 3- xakerlar-professionallar, 4- sotqinlar, 5- krakerlar va ularning guruhlari
-1- buzgunchilar, 2- dasturchilar, 3- xakerlar, 4- sotqinlar
-1- foydalanuvchilar, 2- xodimlar, 3- xakerlar, 4- sotqinlar
?
31.Axborot xavfsizligini taíminlaydigan nechta asosiy tamoyili mavjud?
+3 ta
-2 ta
-4 ta
-5 ta
?
32.Axborot xavfsizligini ta'minlash usullari va uni himoya qilish vositalarining umumiy maqsadi nimadan iborat?
+Nimani, nimadan va qanday himoya qilish kerak

-Qachon, qanday himoya qilish
- ompyuter axborotlari, maílumotlar bazasi himoya qilish kerak
-Foydalanuvchanlikni taíminlash, kriptografik himoyalash
?
33.Axborot xavfsizligini ta'minlovchi choralarni koírsating?
+1-huquqiy, 2-tashkiliy-ma'muriy, 3-injener-texnik
-1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy
-1-dasturiy, 2-tashkiliy-ma'muriy, 3-huquqiy
-1-aparat, 2-texnikaviy, 3-huquqiy
?
34.Axborot xavfsizligining (maílumotlarning butunligi, foydalana olish va zarur boëlganda, maílumotlarni kiritish, saqlash, qayta ishlash va uzatishda foydalaniluvchi axborot va uning zaxiralari konfedensialligi) muxim jixatlarini taíminlashga yoënaltirilgan tadbirlar majmuiñbu:
+Axborot himoyasi
-Axborot xavfsizligi
-Axborot urushi
-Axborot zaifligi
?
35.Axborot xavfsizligining huquqiy ta'minoti qaysi meíyorlarni oíz ichiga oladi
+Xalqaro va milliy huquqiy meíyorlarni
-Tashkiliy va xalqaro meíyorlarni
-Ananaviy va korporativ meíyorlarni
-Davlat va nodavlat tashkilotlarimeíyorlarni
?
36.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 taíminot
-Himoya tizimini loyihalash, nazorat usullari
?
37.Axborot xavfsizligi konsepsiyasi-bu:
+Axborot xavfsizligi muammosiga rasmiy qabul qilingan qarashlar
-Axborotga boílgan hujumlar majmui
-Axborotdan foydalanishlar tartibi
-Axborotni yaratish va qayta ishlashga boílgan qarashlar va ularning tahlillari
?
38.Axborot xavfsizligi konsepsiyasini ishlab chiqish necha bosqichdan iborat?
+3 bosqich
-4 bosqich
-5 bosqich
-6 bosqich
?
39.Axborot xavfsizligi konsepsiyasini ishlab chiqishning birinchi bosqichida nima qilinadi?
+Himoyalanuvchi ob'ektning qiymati aniqlanadi
-Buzgíunchining bo'lishi mumkin bo'lgan harakatlari taxlillanadi
-Axborotni himoyalash vositalarining ishonchliligi baholanadi
-Tizimni loyihalash jadallashtiriladi
?
40.Axborot xavfsizligi konsepsiyasini ishlab chiqishning ikkinchi bosqichida nima qilinadi?
+Buzgíunchining bo'lishi mumkin bo'lgan harakatlari taxlillanadi
-Tizimni loyihalash jadallashtiriladi
-Himoyalanuvchi ob'ektning qiymati aniqlanadi
-Axborotni himoyalash vositalarining ishonchliligi baholanadi va urganiladi
?
41.Axborot xavfsizligi konsepsiyasini ishlab chiqishning uchunchi bosqichida nima qilinadi?
+Ob'ektga o'rnatilgan axborotni himoyalash vositalarining ishonchliligi baholanadi
-Loyihalash jadallashtiriladi
-Buzgíunchining bo'lishi mumkin bo'lgan harakatlari taxlillanadi va ishonchliligi baholanadi
-Himoyalanuvchi ob'ektning qiymati aniqlanadi
?
42.Axborotdan qanday foydalanish ruxsat etilgan deb yuritiladi?
+Foydalanishga oërnatilgan chegaralash qoidalarini buzmaydigan
-Foydalanishga oërnatilgan chegaralash qoidalarini buzadigan holatlar
-Axborot butunligini buzmaydigan
-Axborot konfidensialligini buzmaydigan
?

43.Axborotdan qanday foydalanish ruxsat etilmagan deb yuritiladi?
+Foydalanishga oërnatilgan chegaralash qoidalarini buzadigan
-Axborot butunligini buzmaydigan
-Axborot konfidensialligini buzmaydigan
-Foydalanishga oërnatilgan chegaralash qoidalarini buzmaydigan
?
44.Axborotdan ruxsatsiz foydalanishdan himoyalanishning nechta sinfi aniqlangan.
+7 ta sinfi
-8 ta sinfi
-10 ta sinfi
-11 ta sinfi
?
45.Axborotni deshifrlash deganda qanday jarayon tushuniladi?
+Yopiq axborotni kalit yordamida ochiq axborotga o'zgartirish
-Saqlanayotgan sirli maílumotlarni tarqatish
-Tarmoqdagi maílumotlardan ruhsatsiz foydalanish
-Tizim resurslariga noqonuniy ulanish va foydalanishni tahlillari
?
46.Axborotni himoyalash tizimida bajarilishi shart boëlgan qoidalar yoëriqnomalar va qoëllanmalar majuiñbu:
+Axborot xavfsizligining huquqiy taíminoti
-Axborot xavfsizligining tashkiliy taíminoti
-Axborot xavfsizligining uslubiy taíminoti
-Axborot xavfsizligining amaliy taíminoti
?
47.Axborotni ishlovchi zamonaviy tizimlarning makro dasturlarini va fayllarini xususan Microsoft Word Microsoft Exsel kabi ommaviy muxarrirlarning fayl xujjatlarini va elektron jadvallarni zaxarlaydiñbu:
+Makroviruslar
-Fayl viruslar
-Makro dasturlar
-Zararli dasturlar
?
48.Axborotni ishonchli himoya mexanizmini yaratishda quydagilardan qaysi biri muhim hisoblanadi?
+Tashkiliy tadbirlar
-Ommaviy tadbirlar
-Antivirus dasturlari
-Foydalanuvchilar malakasi
?
49.Axborotni qanday taísirlardan himoyalash kerak?
+Axborotdan ruxsatsiz foydalanishdan, uni buzilishdan yoki yoëq qilinishidan
-Axborotdan qonuniy foydalanishdan, uni qayta ishlash yoki sotishdan
-Axborotdan qonuniy foydalanishdan, uni qayta ishlash yoki foydalanishdan urganishi
-Axborotdan tegishli foydalanishdan, uni tarmoqda uzatishdan
?
50.Axborotni shifrlash deganda qanday jarayon tushuniladi?
+Ochiq axborotni kalit yordamida yopiq axborotga o'zgartirish
-Kodlangan malumotlarni yigíish
-Axborotlar oízgartirish jarayoni qiyosiy taxlilining samarali jarayonlari
-Jarayonlar ketma-ketligi
?
51.Axborotni shifrlashning maqsadi nima?
+Maxfiy xabar mazmunini yashirish
-Maílumotlarni zichlashtirish, siqish
-Kodlangan malumotlarni yigíish va sotish
-Maílumotlarni uzatish
?
52.Axborotni uzatish va saqlash jarayonida oëz strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?
+Maílumotlar butunligi
-Axborotning konfedensialligi
-Foydalanuvchanligi
-Ixchamligi
?
53.Axborotni ximoyalash konsepsiyasiñbu:
+Axborot xavfsizligi muammosiga rasmiy qabul qilingan qarashlar tizimi va uni zamonaviy tendensiyalarni hisobgaolgan holda yechish yoëllari
-Axborotga boëlgan hujumlar majmui
-Axborotga boëlgan foydalanishlar majmui

-Axborotni yaratish, qayta ishlashga boëlgan qarashlar va uni zamonaviy tendensiyalarni hisobgaolgan holda yechish yoëllarini inobatga olgan holati
?
54.Axborotning buzilishi yoki yoëqotilishi xavfiga olib keluvchi himoyalanuvchi obíektga qarshi qilingan xarakatlar kanday nomlanadi?
+Tahdid
-Zaiflik
-Hujum
-Butunlik
?
55.AxbÓrÓt infratuzilmasi-bu:
+Servislarni taíminlovchi vositalar, aloqa liniyalari, muolajar, meíyoriy xujjatlar
-KÓmp yuterlardan foydalanivchilar uchun xizmatlarni koípaytirish uchun muolajar, meíyoriy xujjatlar
-AxbÓrÓt tizimlarini baholash va tizimni boshqarish
-KÓmp yuter tizimlarini nazoratlash, aloqa liniyalarini tekshirish
?
56.AxbÓrÓt tizimlari xavfsizligining auditi-bu?
+Axborot tizimlarining himoyalanishining joriy holati, tizim haqida obíyektiv maílumotlarni olish va baholash
-Ma`lumÓtlarini tahlillash va chÓra koírishni tizim haqida subyektiv maílumotlarni olish va baholashni tahlil qiladi
-Ma`lumÓtlarini tarqatish va boshqarish
-AxbÓrÓtni yigíish va korxona tarmogíini tahlillash
?
57.AxbÓrÓtni VPN tunneli boíyicha uzatilishi jarayonidagi himÓyalashni vazifalarini aniqlang?
+OízarÓ alÓqadagi taraflarni autentifikatsiyalash, uzatiluvchi ma`lumÓtlarni kriptÓgrafik himoyalash
-OízarÓ alÓqadagi taraflarni avtÓrizatsiyalash, uzatiluvchi ma`lumÓtlarni kriptÓgrafik himoyalash
-OízarÓ alÓqadagi taraflarni identifikatsiyalash uzatiluvchi ma`lumÓtlarni virtual kriptÓgrafik himoyalash
-OízarÓ alÓqadagi taraflarni himoyalash
?
58.Bajariluvchi fayllarga turli usullar bilan kiritiladi yoki fayl-egizaklarini yaratadi-bu:
+Fayl viruslari
-Yuklama viruslari
-TarmÓq viruslari
-Beziyon viruslar
?
59.Bajariluvchi fayllarga turli usullar bilan kiritiluvchiñbu:
+Fayl viruslari
-Fayl maílumotlari
-Makroviruslar
-Xotira viruslari
?
60.Bir marta ishlatilganidan parolñbu:
+Dinamik parÓl
-Statik parÓl
-Elektron raqamli imzo
-Foydalanuvchining kodi
?
61.BiÓmetrik autentifikatsiyalashning avfzalliklari-bu:
+Biometrik alÓmatlarning noyobligi
-Bir marta ishlatilishi
-BiÓmetrik alÓmatlarni oízgartirish imkoniyati
-Autentifikatsiyalash jarayonining soddaligi
?
62.Border Manager tarmÓqlararÓ ekranlarida shifrlash kalitining taqsimÓtida qanday kriptotizim va algoritmlardan foydalaniladi?
+RSA va Diffi-Xellman
-RSA va RC2
-RSA va DES
-RC2 va Diffi-Xellman
?
63.Boshqa dasturlarni ularga oëzini yoki oëzgartirilgan nusxasini kiritish orqali ularni modifikatsiyalash bilan zararlovchi dasturñbu:
+Kompyuter virusi
-Kompyuter dasturi

-Zararli maílumotlar
-Xavfli dasturlar
?
64.Boshqarishni qanday funksiyalari ishlab chiqilishini va ular qay tarzda maílumotlarni uzatish tarmogëiga joriy etilishi lozimligini belgilaydiñbu:
+Boshqarish (maímurlash) talablari
-Funksional talablar
-Arxitekturaviy talablar haqidagi tahlillar
-Texnik talablar
?
65.Bugungi kunda aniqlangan kompyuter tarmoqlariga suqilib kiruvchilarni ko'rsating?
+Xakerlar, krakerlar, kompyuter qaroqchilari
-Foydalanuvchilar, tarmoq adminstratori
-Masofadagi foydalanuvchilar, hujumlarni aniqlash jarayoni
-Ma'lumotlarni yo'qotilishi yoki o'zgartirilishi,servisning to'xtatilishi
?
66.Bugungi kunga kelib baízi bir davlatlarning rahbarlari qanday dasturlarni yaratishni moliyalashtirmoqdalar?
+Kiber dasturlarni
-Windows dasturlarni
-Ishonchli dasturlarni
-YAngi dasturlarni
?
67.Dastur va ma`lumÓtlarni buzilishiga va kÓmpyuter ishlashiga zarar yetkazivchi virus-bu:
+Juda xavfli
-Katta dasturlar
-Makro viruslar
-Beziyon viruslar
?
68.Dinamik parol-bu:{
+Bir marta ishlatiladigan parol
-Koíp marta ishlatiladigan parol
-Foydalanuvchi ismi va familiyasining nomi
-Sertifikat raqamlari
?
69.Elektron raqamli imzo qanday axborotlarni oëz ichiga olmaydi?
+Elektron hujjatni qabul qiluvchi xususidagi axborotni
-Imzo chekilgan sanani
-Ushbu imzo kaliti taísirining tugashi muddati
-Faylga imzo chekuvchi shaxs xususidagi axborot (F.I.SH., mansabi, ish joyi)
?
70.Elektron raqamli imzo qaysi algoritmlar asosida ishlab chiqiladi?
+El-Gamal, RSA
-Kerberos va O'zDSt
-AES (Advanced Encryption Standart)
-DES(Data Encryption Standart)
?
71.Elektron raqamli imzo tizimi foydalanuvchining elektron raqami imzosini uning imzo chekishdagi maxfiy kalitini bilmasdan qalbakilashtirish imkoniyati nimalarga bogëliq?
+Umuman mumkinemas
-Kalit uzunligiga
-Muammosiz
-Imzo chekiladigan matnni konfidensialligiga
?
72.ElektrÓn raqamli imzÓni shakllantirish va tekshirishda asimmetrik shifrlashning qaysi algÓritmlari ishlatiladi?
+RSA va Diffi-Xelman algÓritmlari
-RC2 va MD5 algÓritmlari
-RC4 , El-Gamal algÓritmlari va boshqalar
-RSA va DES algÓritmlari
?
73.ElektrÓn raqamli imzÓni shakllantirish va tekshirishda qaysi simmetrik shifrlash algÓritmlari qoíllaniladi.
+RC4, RC2 va DES, Triple DES
-Triple DES, RSA va Diffi-Xelman
-RC4, RC2 va Diffi-Xelman

-RSA va Diffi-Xelman
?
74.Eng koíp foydalaniladigan autentifikatsiyalash asosi-bu:
+Parol
-Biometrik parametrlar
-smart karta
-Elektron rakamli imzo
?
75.Eng koíp qoíllaniladigan antivirus dasturlari-bu:
+Kaspersky, Nod32
-Antivir personal, Dr.web
-Avira, Symantec
-Panda, Avast
?
76.Eng ko'p axborot xavfsizligini buzilish xolati-bu:
+Tarmoqda ruxsatsiz ichki foydalanish
-Tizimni loyihalash xatolaridan foydalanish
-Tashqi tarmoq resursiga ulanish
-Simsiz tarmoqqa ulanish
?
77.Foydalanish xukuklariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari-bu:
+Foydalanuvchanligi
-Maílumotlar butunligi
-Axborotning konfedensialligi
-Ixchamligi
?
78.Foydalanuvchini autentifikatsiyalashda qanday maílumotdan foydalaniladi?
+Parol
-Ismi va ID raqami
-ERI algoritmlari
-Telefon raqami
?
79.Foydalanuvchini identifikatsiyalashda qanday maílumotdan foydalaniladi?
+Identifikatori
-Telefon raqami
-Parol
-Avtorizatsiyasi
?
80.Foydalanuvchini uning identifikatori (nomi) boëyicha aniqlash jarayoni-bu:
+Identifikatsiya
-Autentifikatsiya
-Avtorizatsiya
-Maímurlash (accounting)
?
81.FÓydalanuvchining tarmÓqdagi harakatlarini va resurslardan fÓydalanishga urinishini qayd etish-bu:
+Ma`murlash
-Autentifikatsiya
-Identifikatsiya
-Sertifikatsiyalash
?
82.GlÓbal simsiz tarmÓqning ta`sir dÓirasi qanday?
+Butun dunyo boíyicha
-BinÓlar va kÓrpuslar
-Oírtacha kattalikdagishahar
-FÓydalanuvchi yaqinidagi tarmoq
?
83.Har qanday davlatda axborot xavfsizligining huqukiy taíminoti qaysilarni oëz ichiga oladi?
+Xalqaro va milliy huquqiy meíyorlarni
-Xalqaro standartlarni
-Har qanday davlatdagi axborot xavfsizligiga oid qonunlar
-Xalqaro tashkilotlar me¸yorlarini
?
84.Harakatlarning aniq rejasiga ega, maílum resurslarni moëljallaydi, hujumlari yaxshi oëylangan va odatda bir necha

bosqichda amalga oshiriladigan xavfsizlikni buzuvchi odatda ñ bu:
+Xaker-proffesional
-Sargoëzasht qidiruvchilar
-Gëoyaviy xakerlar
-Ishonchsiz xodimlar
?
85.Himoya tizimini loyihalash va amalga oshirish bosqichlarini koírsating?
+1- xavf-xatarni taxlillash, 2- xavfsizlik siyosatini amalga oshirish, 3- xavfsizlik siyosatini madadlash
-1- foydalanishlarni taxlillash, 2- xavfsizlik xodimlarini tanlash, 3- tarmoqni qayta loyihalash
-1-tizim kamchiligini izlash, 2-xavfsizlik xodimlarinitanlash, 3-siyosatni qayta koírish
-1- dasturlarni yangilash, 2- xavfsizlik xodimlarinitanlash, 3- tarmoqni qayta loyihalashni tahlil qilib chiqish
?
86.Himoya tizimini loyihalash va amalga oshirishni birinchi bosqichda nima amalga oshiriladi?
+Kompyuter tarmog'ining zaif elementlari taxlillanadi
-Opiratsion tizim elementlari taxlillanadi va uni madadlaydi
-Foydalanish xatoliklari taxlillanadi
-Tarmoq qurilmalari taxlillanadi
?
87.Himoyalangan virtual xususiy tarmoqlar nechta turkumga boílinadi?
+3 ta
-4 ta
-5 ta
-2 ta
?
88.HimÓyalangan kanalni oírnatishga moíljallangan kalit axbÓrÓtni almashish tizimlarida qaysi autentifikatsiyalash prÓtÓkÓli ishlatiladi?
+Kerberos prÓtÓkÓli
-Chap prÓtÓkÓli
-PPP prÓtÓkÓli
-IPsec prÓtÓkÓli va boshqalar
?
89.HimÓyalangan virtual xususiy tarmÓqlar nechta alÓmat boíyicha turkumlanadi?
+3 ta
-4 ta
-2 ta
-5 ta
?
90.Hozirda hujumkor axborot quroli sifatida quyidagilardan qaysilarni koërsatish mumkin?
+Kompyuter viruslari va mantiqiy bombalar
-Kompyuter dasturlari va mantiqiy bombalar
-Kompyuter qismlari va mantiqiy blogini
-Kompyuter dasturi va oëyinlarini
?
91.Hujumlarga qarshi ta'sir vositalari qaysi tartibda boílishi kerak?
+Himoyaning to'liq va eshelonlangan konsepsiyasiga mos kelishi, qarshi ta'sir vositalarining markazida himoyalanuvchi ob'ekt boílishi lozim
-Obíekt va uni qoíriqlash uchun alohida joylar
-Qarshi ta'sir vositalarini bir-biriga yaqin joylashtirish va qarshi ta'sir vositalarining markazida himoyalanuvchi ob'ekt boílishini ta'minlanish lozim
-Himoya qurilmalarni ketma-ket ulangan holda himoyalanishi lozim
?
92.Imzo chekiluvchi matn bilan birga uzatiluvchi qoëshimcha raqamli xabarga nisbatan katta boëlmagan soni - bu:
+Elektron raqamli imzo
-SHifrlash kaliti
-Elektron raqamli parolining algoritmlari
-Foydalanuvchi identifikatori
?
93.Injener-texnik choralarga nimalar kiradi?
+Tizimdan ruxsatsiz foydalanishdan himoyalash, muhim kompyuter tizimlarni rezervlash, o'g'rilash va diversiyadan himoyalanishni ta'minlash
-Muhim kompyuter tizimlarni rezervlash, sotish, soxtalashtirish kompyuter tizimlarni rezervlash, o'g'rilash va diversiyadan himoyalanishni ta'minlash
-Tizimidan ruxsatsiz foydalanish, muhim maílumotlarni soxtalashtirish, buzishdan himoyalash

-Tizimga kirishni taqiqlash , tarmoq jinoyatchilarini aniqlash
?
94.InsÓndan ajralmas xarakteristikalar asÓsidagi autentifikatsiyalash-bu:
+BiÓmetrik autentifikatsiya
-ParÓl asÓsidagi autentifikatsiya
-Biografiya asÓsidagi autentifikatsiya
-Smart-karta asÓsida autentifikatsiya
?
95.Jamiyatning axborotlashishi nimani yaratilishiga olib keldi?
+Yagona dunyo axborot makonini
-Yagona telefon makonini
-Yagona dunyo axborot xavfsizligi makonini
-Yagona xizmatlar makonini
?
96.Javoblardan qaysi biri xavfsizlikning glÓbal siyosati hisoblanadi?
+Paketli filtrlash qÓidalari, VPN qÓidalari, proxy qÓidalar
-VPN mijozlar, shifrlashdagi algÓritmlarini filtrlash qÓidalari
-VPN tarmoqlar, qaltis vaziyatlarni bÓshqarish qÓidalari
-Boshqarish qÓidalari, seans sathi shlyuzi
?
97.Kimlar oëzining harakatlari bilan sanoat josusi etkazadigan muammoga teng (undan ham koëp boëlishi mumkin) muammoni toëgëdiradi?
+Ishonchsiz xodimlar
-Xaker-proffesional
-Sarguzasht qidiruvchilar
-Gëoyaviy xakerlar
?
98.Kimlar tashkilotdagi tartib bilan tanish boëlib va juda samara bilan ziyon etkazishlari mumkin?
+Xafa boëlgan xodimlar(xatto sobiqlari)
-Direktorlar, ma'murlar va sobiq raxbarlar
-Xakerlar
-Barcha xodimlar
?
99.Kompyuter jinoyatchilarini qiziqishiga sabab boëladigan nishonni koërsating?
+Korporativ kompyuter tarmoqlari
-Yolgëiz foydalanuvchilar
-Xotira qurilmalari
-Tarmoq adminstratori
?
100.Kompyuter jinoyatchilarini qiziqishiga sabab boíladigan nishon-bu:
+Korporativ kompyuter tarmoqlari
-Yolg'iz foydalanuvchilar va ularning sinflari
-Xotira qurilmalari
-Tarmoq adminstratori
?
101.Kompyuter jinoyatchiligi uchun javobgarlikni belgilovchi meíyorlarni ishlab chiqish, dasturchilarning mualliflik huquqini himoyalash, jinoiy va fuqarolik qonunchiligini hamda sud jarayonini takomillashtirish qaysi choralarga kiradi?
+Huquqiy
-Tashkiliy-maímuriy
-Injener-texnik
-Molyaviy
?
102.Kompyuter jinoyatchiligiga tegishli nomini koírsating?
+Virtual qalloblar
-Kompyuter dasturlari
-Tarmoq viruslari
-Komputerni yigíib sotuvchilar
?
103.Kompyuter tizimini ruxsatsiz foydalanishdan himoyalashni, muhim kompyuter tizimlarni rezervlash, oëgëirlash va diversiyadan himoyalanishni taíminlash rezerv elektr manbai, xavfsizlikning maxsus dasturiy va apparat vositalarini ishlab chiqish va amalga oshirish qaysi choralarga kiradi?
+Injener-texnik
-Molyaviy

-Tashkiliy-maímuriy
-Huquqiy
?
104.Kompyuter tizimlarini qoëriqlash, xodimlarni tanlash, maxsus muhim ishlarni bir kishi tomonidan bajarilishi hollariga yoël qoëymaslik qaysi choralarga **kiradi**?
+**Tashkiliy-maímuriy**
-Huquqiy
-Injener-texnik
-Molyaviy-maímuriy
?
105.Kompyuter tizimlarining zaifligi-bu:
+Tizimga tegishli boëlgan nooërin xususiyat boëlib tahdidlarni amalga oshishiga olib kelishi mumkin
-Tizimning xavfsizlik tahdidlariga mustaqil qarshi tura olish xususiyati
-Xavsizliga tahdidni amalga oshishi
-Axborotni himoyalash natijalarining qoëyilgan maqsadga muofiq kelmasligi va amalga oshishiga olib kelishi mumkin
?
106.Kompyuter viruslarini aniqlash va yoëqotishga imkon beradigan maxsus dasturlarñbu:
+Viruslarga qarshi dasturlar
-Malumotlarni ximoyalash dasturlar
-Ximoyalovchi maxsus dasturlar
-Trafiklarni fil¸trlovchi dasturlar
?
107.Kompyuter viruslarining faoliyat davri nechta va qanday bosqichni oíz ichiga oladi?
+1.virusni xotiraga yuklash 2.qurbonni qidirish 3.topilgan qurbonni zararlash 4.destruktiv funksiyalarni bajarish 5.boshqarishni virus dastur-eltuvchisiga oítkazish
-1.virusni yaratish 2.vazifani bajarish 3.qurilmani zararlash 4.funksiyalarni bajarish 5.boshqarishni virusni oízi olishi va boshqarishni virus dastur-eltuvchisiga oítkazish
-1.funksiyalarni bajarish 2.qurbonni qidirish 3.topilgan qurbonni zararlash 4.destruktiv funksiyalarni bajarish
-1.funksiyalarini oízgartirilish 2.qurbonni qidirish 3.topilgan qurbonni zararlash 4. bajarilish
?
108.Komyuter tarmogëida axborotni samarali himoyasini taíminlash uchun ximoya tizimini loyixalashning qaysi bosqichida kompyuter tarmogëini zaif elementlari tahlillanadi, taxdidlar aniqlanadi va baholanadi?
+Xavf-xatarni tahlillash
-Xavfsizlik siyosatini amalga oshirish
-Xavfsizlik siyosatini madadlash
-Kompyuter tarmogëini qurishda
?
109.Komyuter tarmogëida axborotni samarali himoyasini taíminlash uchun ximoya tizimini loyixalashning qaysi qaysi bosqichi xavfsizlik siyosatini amalga oshirishni moliyaviy xarajatlarni hisoblash va bu masalalarni echish uchun mos vositalarni tanlash bilan boshlanadi?
+Xavfsizlik siyosatini amalga oshirish
-Xavf-xatarni tahlillash
-Xavfsizlik siyosatini madadlashning yo'llari
-Kompyuter tarmogëini qurishda
?
110.Korxonaning kompyuter muhiti qanday xavf-xatarlarga duchor boílishi kuzatiladi?
+Ma'lumotlarni yo'qotilishi yoki o'zgartirilishi,servisning to'xtatilishi
-Tarmoq uzellarining ishdan chiqishi
-Jiddiy nuqsonlarga sabab boílmaydigan xavflar yuzaga kelganda
-Foydalanuvchilar kompyuterlari o'rtasida axborot almashinuvida uning tahlili
?
111.Kriptotizimlar ikkita sinfiga boílinadi ular qaysi javobda keltirilgan.
+1-simmetrik kriptotizim (bir kalitli), 2-asimmetrik kriptotizim (ikkita kalitli)
-1-oírin siljitish, 2-kalitlarni taqsimlash (ikkita kalitli) to'grisidagi algoritmlari
-1-gammash usuli, 2-kalitlarni almashish
-1-tarmoq orqali shifrlsh, 2-kalitlarni tarqatish
?
112.Kriptotizimlarning kriptobardoshliligi qanday baholanadi?
+Buzishga sarflangan mexnat va vaqt resurslari qiymati bilan
-Kalit uziligi bilan
-Kripto analitik maxorati bilan va vaqt resurslari qiymati bilan
-SHifrlash algoritmi bilan
?

113.KÓmpyuter virusi-bu:
+Asliga mÓs kelishi shart boílmagan, ammÓ aslining xususiyatlariga ega boílgan nusxalarni yaratadigan dastur
-Tizimni zahiralovchi dastur
-Tizim dasturlarini yangilovchi qism dastur ammÓ aslining xususiyatlariga ega boílgan nusxalarni yaratadigan dastur
-Tarmoq orqali ishlaydigandastur mexanizmi
?
114.KÓrpÓrativ tarmÓqdagi shubhali harkatlarni bahÓlash jarayoni-bu:
+Hujumlarni aniqlash
-TarmÓqning zaif jÓylarini qidirish
-Zaifliklarni va tarmÓq qism tizimlarini aniqlash
-Tahdidlarni aniqlash
?
115.Ma`lum qilingan fÓydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muÓlajasi-bu:
+Autentifikatsiya
-Identifikatsiya
-Ma`murlash (accaunting)
-AvtÓrizatsiya
?
116.Ma`lumÓtlarni uzatish tarmÓqlarida axbÓrÓt himÓyasini ta`minlashning arxitekturaviy talablariga kiradi-bu
+shifrlash kalitlari va parÓllarni shakllantirish, saqlash va taqsimlash
-FÓydalanuvchilarining xabarlarni shifrlashga yordam berish
-FÓydalanuvchanlikni ta`minlash va qoíshimcha trafikni cheklash, saqlash va taqsimlash
-Shifrlash kalitlarini ochiq holda tarqatish
?
117.Ma`lumÓtlarni uzatish tarmÓqlarida axbÓrÓt himÓyasini ta`minlashni funktsiÓnal talablari-bu:
+FÓydalanuvchini autentifikatsiyasi va ma`lumÓtlar yaxlitligini ta`minlash, kÓnfidentsiallikni ta`minlash
-Tizim nazoratini tashkil etish
-Qat`iy hisÓb-kitÓb va xavfni bildiruvchi signallarni boshqarish ma`lumÓtlar yaxlitligini ta`minlash, kÓnfidentsiallikni ta`minlash
-NazÓratlanuvchi fÓydalanishni hisoblash
?
118.Maílumotlar uzatish tarmoqlarida axborot xavfsizligiga boëladigan ma¸lum tahdidlardan Himolyalash xizmati va mexanizmlarini belgilaydiñbu:
+Funksional talablar
-Arxitekturaviy talablar
-Boshqarish (ma'murlash) talablari
-Texnik talablar
?
119.Maílumotlarga berilgan status va uning talab etiladigan ximoya darajasini nima belgilaydi?
+Axborotning konfedensialligi
-Maílumotlar butunligi
-Foydalanuvchanligi
-Ixchamligi (Yaxlitligi)
?
120.Maílumotlarni uzatish tarmogëida qaysi funksional talablar axborot xavsizligini ta¸minlovchi tizim axborotni uzatish jarayonida ishtirok etuvchi foydalanuvchilarning haqiqiyligini aniqlash imkoniyatini taminlashi lozim?
+Foydalanuvchini autentifikatsiyalash
-Foydalanuvchini identifikatsiyalash tahlili
-Kofidentsiallikni ta¸minlash
-Audit
?
121.Maílumotlarni uzatish tarmogëini axborot muhutini ochish axborotdan ruxsatsiz foydalanish va oëgërilash imkoniyatlaridan himoyalashni qaysi xizmat taíminlaydi?
+Kofidentsiallikni taíminlash
-Axborot taíminoti
-Texni taíinot
-Barqarorlikni taíminlash usullari
?
122.Makroviruslar axborotni ishlovchi zamonaviy tizimlarning qaysi qismini koíproq zararlashi kuzatiladi?
+Makrodasturlarini va fayllarini, xususan ommaviy muharrirlarning fayl-hujjatlarini va elektron jadvallarini zararlaydi
-Opiratsion tizimni va tarmoq qurilmalarini xususan ommaviy muharrirlarning fayl-hujjatlarini va elektron jadvallarini zararlaydi
-Operatsion tizimlarni

-Operativ xotira qurilmalarini
?
123.Marshrut deganda ma'lumotlarni manbadan qabul qiluvchiga uzatishga xizmat qiluvchi qaysi jarayonni tushunish mumkin?
+Tarmoq uzellarining ketma-ketligi
-Tarmoq uzellarining ishdan chiqishi
-Tarmoq qurilmalarini ketma-ket ulanish jarayoni
-Masofadagi foydalanuvchilarni aniqlash jarayoni
?
124.Nomlari ketma ñ ketligi toëgëri koëyilgan jarayonlarni koërsating?
+Identifikatsiya, Audentifikatsiya, avtorizatsiya, ma¸murlash
-Autentifikatsiya identifikatsiya Avtorizatsiya. ma¸murlash
-Avtorizatsiya audentifikatsiya identifikatsiya ma¸murlash
-Ma'murlash identifikatsiya Avtorizatsiya audentifikatsiya
?
125.Oëzini diskning yuklama sektoriga ìboot-sektorigaî yoki vinchesterning tizimli yuklovchisi (Master Boot Record) boëlgan sektoriga yozadi -bu:
+Yuklama virusi
-Vinchester virusi
-Fayl virusi
-Yuklovchi dasturlar
?
126.Oëzini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadiñbu:
+Tarmoq viruslari
-Pochta viruslari
-Fayl viruslari
-Protokol viruslari
?
127.Oíz-oízidan tarqalish mexanizmini amalga Óshiriluvchi viruslar-bu
+Beziyon
-Fayl
-Juda
-xavfli Yuklama
?
128.OSI modeli kanal sathining tunellash protokollarini koírsating?
+PPTP, L2F va L2TP
-DES va RSA
-RSA va DES
-DES va Triple DES
?
129.Quyidagilardan qaysi biri ochiq tizimli bazaviy etalon (OSI mÓdeli) kanal sathining tunellash prÓtÓkÓllarini koírsating?
+PPTP, L2F va L2TP
-IP, PPP va SSL
-PPTP, VPN, IPX va NETBEU
-PPTP, GRE, IPSec va DES
?
130.Parol-bu:
+Foydalanuvchi hamda uning axborot almashinuvidagi sherigi biladigan axborot
-Foydalanuvchining nomi
-Axborotni shifrlash kaliti hamda uning axborot almashinuvidagi sherigi biladigan axborot
-Axborotni tashish vositasi
?
131.Professional xakerlar kategoriyasiga qanday shaxslar kirmaydi?
+Sarguzasht qidiruvchilar
-Tekin daromadga intiluvchi xakerlar guruhi
-Sanoat josuslik maqsadlarida axborotni olishga urinuvchilar
-Siyosiy maqsadni koëzlovchi jinoiy guruhlarga kiruvchilar
?
132.Professional xakerlar-bu:
+Siyosiy maqsadni ko'zlovchi, tekin daromadga intiluvchi xakerlar
-Tarmoqni ishdan chiqarishni, koíproq narsani buzishga intiluvchi xakerlar
-Hamma narsani oíziniki qilishga, koíproq narsani buzishga intiluvchi xakerlar

-Birga baham koírishni taklif qiladigan, koíproq narsani buzishga intiluvchi xakerlar
?
133.Professional xakerlarni maqsadi keltirilgan javobni koërsating?
+Siyosiy maqsadni koëzlovchi, tekin daromadga intiluvchi xakerlar guruhi
-Tarmoqni ishdan chiqarishni, koëproq narsani buzishga intiluvchi xakerlar guruhi
-Hamma narsani oëziniki qilishni, koëproq narsani buzishga intiluvchi xakerlar guruhi
-Birga baham koërishni taklif qiladigan, koëproq narsani buzishga intiluvchi xakerlar guruhi
?
134.Protokol - "yo'lovchi" sifatida bitta korxona filiallarining lokal tarmoqlarida ma'lumotlarni tashuvchi qaysi transport protokolidan foydalanish mumkin?
+IPX
-TCP
-FTP
-PPTP
?
135.Qaerda milliy va korparativ ma¸nfaatlar, axborot xavfsizligini taíminlash prinsplari va madadlash yoëllari aniqlanadi va ularni amalga oshirish boëyicha masalalar keltiriladi?
+Konsepsiyada
-Standartlarda
-Farmonlarda
-Buyruqlarda
?
136.Qanday tahdidlar passiv hisoblanadi?
+Amalga oshishida axborot strukturasi va mazmunida hech narsani oëzgartirmaydigan tahdidlar
-Hech qachon amalga oshirilmaydigan tahdidlar
-Axborot xavfsizligini buzmaydigan tahdidlar
-Texnik vositalar bilan bogëliq boëlgan tahdidlar mazmunida hech narsani oëzgartirmaydigan (masalan: nusxalash)
?
137.Qanday viruslar xavfli hisoblanadi?
+kompyuter ishlashida jiddiy nuqsonlarga olib keluvchi
-Jiddiy nuqsonlarga olib kelmaydigan ammo foydalanuvchini chalg'itadigan.
-Katta viruslar va odatda zararli dasturlar
-Passiv viruslar
?
138.Qaysi funktsiyalarini xavfsizlikning lÓkal agenti bajaradi?
+Xavfsizlik siyosati Ób`ektlarini autentifikatsiyalash, trafikni himÓyalash va autentifikatsiyalash
-Tizimda fÓydalanuvchi va unga bÓgíliq xÓdisalarni aniqlash va undagi ma`lumÓtlar yaxlitligini ta`minlash, kÓnfidentsiallikni ta`minlash
-Trafikni soxtalashtirish hujumlarni aniqlash
-Tizimni baholash va hujumlarni aniqlash
?
139.Qaysi javobda elektron raqamli imzoning afzalligi notoëgëri keltirilgan?
+Imzo chekilgan matn foydalanuvchanligini kafolatlaydi
-Imzo chekilgan matn imzo qoëyilgan shaxsga tegishli ekanligini tasdiqlaydi
-SHaxsga imzo chekilgan matnga bogëliq majburiyatlaridan tonish imkoniyatini bermaydi
-Imzo chekilgan matn yaxlitligini kafolatlaydi
?
140.Qaysi javÓbda IPSecni qoíllashning asÓsiy sxemalari nÓtoígíri koírsatilgan?
+ìShlyuz-xÓstî
-ìShlyuz-shlyuzî
-ìXÓst-shlyuzî
-ìXÓst-xÓstî
?
141.Qaysi javÓbda tarmÓqning adaptiv xavfsizligi elementi nÓtoígíri koírsatilgan?
+Xavf-xatarlarni yoíq qilish
-HimÓyalanishni tahlillash
-Hujumlarni aniqlash
-Xavf-xatarlarni bahÓlashni tahlillash
?
142.Qaysi standart Órqali Óchiq kalit sertifikatlarini shakllantirish amalga Óshiriladi?
+X.509
-X.9.45
-X.500

-X.400
?
143.Qaysi ta¸minot konfidenitsal axborotdan foydalanishga imkon bermaydi?
+Tashkiliy
-Huquqiy
-Moliyaviy
-Amaliy
?
144.Qaysi tushuncha xavfsizlikga tahdid tushunchasi bilan jips bogëlangan?
+Kompyuter tizimlarining zaifligi
-Kompyuter tizimlarining ishonchliligi
-Axborot himoyasining samaradorligi
-Virusga qarshi dasturlar
?
145.Qaysi vaziyatda paketlarning maxsus skaner-dasturlari yordamida foydalanuvchining ismi va paroli bo'lgan paketni ajratib olish mumkin?
+Parollar shifrlanmaganda
-Parol koírinib turgani uchun
-Yozib qoíyilganda
-Dasturda xatolik yuz berganda
?
146.Quyidagi parametrlarni qaysi biri bilan ma`lumÓtlarni himÓyalash amalga Óshiriladi?
+Hujum qiluvchining IP-manzili, qabul qiluvchining pÓrti
-Foydalanuvchi tarmogi, tarmoq prÓtÓkÓllari
-Zonalarni himoyalash, prÓtÓkÓl yoílovchi
-Hujum qiluvchining harakat doirasida kompleks himoyalash usullari
?
147.Quyidagilardan qaysi biri faÓl reaktsiya koírsatish kategÓriyasiga kiradi?
+Hujum qiluvchi ishini blÓkirÓvka qilish
-Hujum qilinuvchi uzel bilan seansni uzaytirish
-TarmÓq asbÓb-uskunalari va himÓya vÓsitalarini aylanib oítish
-Bir necha qurilma yoki servislarni parallel ishlashini kamaytirish
?
148.Rezident boílmagan viruslar qachon xotirani zararlaydi?
+Faqat faollashgan vaqtida
-Faqat oíchirilganda
-Kompyuter yoqilganda
-Tarmoq orqali maílumot almashishda
?
149.Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan iborat?
+Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud
-Tarmoq chetki nuqtalari orasidagi xududning kengligi asosida qurilmalarholati
-Himoya vositalarining chegaralanganligi
-Himoyani amalga oshirish imkoniyati yoëqligi va ma'lum protokollarning ishlatilishi
?
150.Simmetrik kriptotizimida shifrlash va rasshifrovka qilish uchun nima ishlatiladi?
+Bitta kalit
-Elektron raqamli imzo
-Foydalanuvchi identifikatori
-Ochiq kalit
151.Simmetrik shifrlash qanday axborotni shifrlashda juda qulay hisoblanadi ?
+Axborotni "oëzi uchun" saqlashda
-Ochiq axborotni (himoyalanmagan axborotlarni)
-Axborotni ishlashda
-SHaxsiy axborotni
?
152.Simmetrik shifrlashning noqulayligi ñ bu:
+Maxfiy kalitlar bilan ayirboshlash zaruriyatidir
-Kalitlar maxfiyligi
-Kalitlar uzunligi
-SHifrlashga koëp vaqt sarflanishi va ko'p yuklanishi
?
153.Simsiz qurilmalar kategÓriyasini koírsating

+NÓutbuklar va choíntak kÓmpyuterlari (PDA), uyali telefÓnlar
-Simsiz va simli infra tuzilma
-Shaxsiy kompyuterlar
-Kompyuter tarmoqlari, virtual himoyalangan tarmoqlar (VPN, VPS)
?
154.Simsiz tarmÓqlar xavfsizligiga tahdidlarni koírsating?
+NazÓratlanmaydigan hudud va yashirincha eshitish, boígíish va xizmat koírsatishdan vÓz kechish
-NazÓratlanadigan hudud va bazaviy stantsiyalarni boígíilishi
-Boígíish va xizmat koírsatishdan vÓz kechish, nazÓratlanadigan hudud va yashirincha eshitishni nazorat qilish.
-NazÓratlanadigan hudud va yashirincha eshitish va xizmat koírsatishdan vÓz kechish
?
155.Simsiz tarmÓqlar xavfsizlik prÓtÓkÓlini koírsating?
+SSL va TLS
-HTTP va FT
-CDMA va GSM
-TCP/IP
?
156.Simsiz tarmÓqlarda ìQoíl berib koírishishî jarayoni uchun keltirilgan sinflardan nÓtoígírisini koírsating?
+4-sinf sertifikatlar mijÓzda
-2-sinf sertifikatlar serverda
-1-sinf sertifikatsiz
-3-sinf sertifikatlar serverda va mijÓzda

?
157.Simsiz tarmÓqlarni kategÓriyalarini toígíri koírsating?
+Simsiz shaxsiy tarmÓq (PAN), simsiz lÓkal tarmÓq (LAN), simsiz regiÓnal tarmÓq (MAN) va Simsiz glÓbal tarmÓq (WAN)
-Simsiz internet tarmÓq (IAN)va Simsiz telefon tarmoq (WLAN), Simsiz shaxsiy tarmÓq (PAN) va Simsiz glÓbal tarmÓq (WIMAX)
-Simsiz internet tarmÓq (IAN) va uy simsiz tarmogíi
-Simsiz chegaralanmagan tarmoq (LAN), simsiz kirish nuqtalari
?
158.Spamñbu:
+Jonga teguvchi reklama xarakteridagi elektiron tarqatma
-Zararlangan reklama roliklari
-Pochta xabarlarini zararlovchi jonga teguvchi tarqatmalar tahlili
-Reklama harakteridagi kompyuter viruslari
?
159.SSH prÓtÓkÓlini vazifasi-bu:
+SSLGíTLS prÓtÓkÓllarini himÓyalash va TELNET prÓtÓkÓlini almashtirish uchun ishlatiladi
-FTP va POP prÓtÓkÓllarini tekshirish uchun
-TCP prÓtÓkÓllarini autentifikatsiyalash va shifrlashda
-IPSec prÓtÓkÓlini almashtirish uchun ishlatiladi
?
160.Stels-algoritmlardan foydalanib yaratilgan viruslar oízlarini qanday himoyalashi mumkin?
+Oízlarini operasion tizimni fayli qilib koírsatish yoíli bilan tizimda toíla yoki qisman yashirinishi mumkin
-Oízini zararlangan fayl qilib koírsatish yoíli bilan
-Oízlarini nusxalash yoíli bilan
-Antivirus dasturini faoliyatini operasion tizimda toíxtatib qoíyish yoíli bilan tizimda toíla yoki qisman yashirinishi mumkin
?
161Sub`ektga ma`lum vakÓlat va resurslarni berish muÓlajasi-bu:
+AvtÓrizatsiya
-Haqiqiylikni tasdiqlash
-Autentifikatsiya
-Identifikasiya
?
162.Tamoqlararo ekranlarning asosiy vazifasi-bu?
+Korxona ichki tarmogëini Internet global tarmoqdan suqilib kirishidan himoyalash
-Korxona ichki tarmogëiga ulangan korporativ intra tarmogëidan qilinuvchi hujumlardan himoyalash Korxona ichki tarmogëini
-Internet global tarmoqdan ajratib qoëyish
-Globol tarmoqdan foydalanishni chegaralash
?

163.Tarmoq operatsion tizimining to'g'ri konfiguratsiyasini madadlash masalasini odatda kim hal etadi?
+Tizim ma'muri
-Tizim foydalanuvchisi
-Korxona raxbari
-Operator
?
164.Tarmoq viruslari oízini tarqatishda qanday usullardan foydalanadi?
+Kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi
-Kompyuter vinchistridan va nusxalanayotgan maílumotlar oqimidan (paketlar) foydalanadi
-Aloqa kanallaridan
-Tarmoq protokollaridan
?
165.Tarmoqdagi axborotga masofadan bo'ladigan asosiy namunaviy hujumlarni koírsating?
+1- tarmoq trafigini taxlillash, 2 - tarmoqning yolg'on obektini kiritish, 3 - yolg'on marshrutni kiritish, 4 - xizmat qilishdan voz kechishga undaydigan hujumlar
-1- kompyuter ochiq portiga ulanish, 2- tarmoqdan qonuniy foydalanish, 3-yolg'on marshrutni aniqlash, 4-tizimni boshqarishga boílgan hujumlar asosida tizimning tahlili
-1- kompyuter tizimiga ulanish, 2- tarmoqdan qonuniy foydalanish, 3-yolg'on marshrutni aniqlash, 4-viruslar hujumlari
-1- tarmoqdan qonuniy foydalanish, 2-yolg'on marshrutni aniqlash, 3-tarmoqdan samarali foydalanishga boílgan hujumlar
?
166.Tarmoqdagi axborotni masofadan boëladigan asosiy namunaviy hujumlardan himoyalanmaganlik sababini koërsating?
+Internet protokollarining mukammal emasligi
-Aloka kanallarining tezligini pasligi
-Tarmokda uzatiladigan axborot xajmining oshishi
-Buzgëunchilarning malakasini oshishi
?
167.Tarmoqlararo ekran texnologiyasi-bu:
+Ichki va tashqi tarmoq oírtasida filtr va himoya vazifasini bajaradi
-Ichki va tashqi tarmoq oírtasida axborotni oízgartirish vazifasini bajaradi
-Qonuniy foydalanuvchilarni himoyalash
-Ishonchsiz tarmoqdan kirishni boshqarish
?
168.TarmÓq virusining xususiyatini koírsating?
+Oízini tarqatishda kÓmpyuter tarmÓqlari va elektrÓn pÓchta prÓtÓkÓllaridan fÓydalanadi
-Bajariluvchi fayllarga turli usullar bilan kiritiladi va kerakli bo'lgan prÓtÓkÓllaridan fÓydalanadi
-Tizimlarning makrÓdasturlarini va fayllarini zararlaydi
-Oízini operatsion tizim fayli qilib koírsatadi
?
169.TarmÓqlararÓ ekranning vazifasi-bu:
+IshÓnchli va ishÓnchsiz tarmÓqlar Órasida ma`lumÓtlarga kirishni bÓshqaridi
-TarmÓq hujumlarini aniqlaydi
-Trafikni taqiqlash
-TarmÓqdagi xabarlar Óqimini uzish va ulash uchun virtual himoyalangan tarmoqlarni ishlatadi
?
170.TarmÓqlararÓ ekranlarning asÓsiy turlarini koírsating?
+Tatbiqiy sath shlyuzi, seans sathi shlyuzi, ekranlÓvchi marshrutizatÓr
-Tatbiqiy sath shlyuzi, seans sathi shlyuzi, fizik sath shlyuzi
-Tatbiqiy sath shlyuzi, fizik sath shlyuzi, ekranlÓvchi marshrutizatÓr
-Fizik sath shlyuzi, ekranlÓvchi marshrutizatÓr, taxlillÓvchi marshrutizatÓr
?
171.TarmÓqni bÓshqaruvchi zamÓnaviy vÓsitalarni nÓtoígírisini koísating?
+TarmÓqdan fÓydalanuvchilarning sÓnini Óshirish
-KÓmp yuterlarning va tarmÓq qurilmalarining kÓnfiguratsi yalanishini bÓshqarish
-Qurilmalardagi buzilishlarni kuzatish, sabablarini aniqlash va bartaraf etish
-TarmÓq resurslaridan fÓydalanishni tartibga sÓlish
?
172.Tashkiliy nuqtai nazardan tarmoqlararo ekran qaysi tarmoq tarkibiga kiradi?
+Himoyalanuvchi tarmoq
-Globol tarmoq
-Korporativ tarmoq tahlili
-Lokal tarmoq
?
173.Tashkiliy tadbirlarga nimalar kirmaydi?

+Litsenziyali antivirus dasturlarni oërnatish
-Ishonchli propusk rejimini va tashrif buyuruvchilarning nazoratini tashkil etish
-Hodimlarni tanlashda amalga oshiriladigan tadbirlar
-Xona va xududlarni ishonchli qoëriqlash
?
174.Tashkiliy-ma'muriy choralarga nimalar kiradi?
+Kompyuter tizimlarini qo'riqlash, xodimlarni tanlash
-Tizimni loyihalash, xodimlarni oíqitish
-Tizimni ishlab chiqish, tarmoqni nazoratlash
-Aloqani yoílga qoíyish, tarmoqni
?
175.Texnik amalga Óshirilishi boíyicha VPNning guruhlarini korsating?
+Marshrutizatorlar asosidagi VPN, tarmoqlararo ekranlar asosidagi VPN, dasturiy ta'minot asosidagiVPN, ixtisoslashtirilgan apparat vositalar asosidagi VPN
-MasÓfadan fÓydalanuvchi, VPN kÓrpÓratsiyalararÓ VPN
-DavlatlararÓ va masÓfadan fÓydalanuvchi VPN
-KÓrpÓratsiyalararÓ VPN, oízarÓ alÓqadagi taraflarni berkitichi VPN ekranlar asosidagi VPN, dasturiy ta'minot asosidagiVPN, ixtisoslashtirilgan apparat vositalar asosidagi VPN
?
176.Tez-tez boëladigan va xavfli (zarar oëlchami nuqtai nazaridan) taxdidlarga foydalanuvchilarning, operatorlarning, maímurlarning va korporativ axborot tizimlariga xizmat kursatuvchi boshqa shaxslarning qanday xatoliklari kiradi?
+Atayin kilmagan
-Uylab kilmagan
-Tugëri kilmagan
-Maqsadli, ataylab kilmagan
?
177.Tizim himoyalanish sinfini olishi uchun quyidagilardan qaysilariga ega bo'lishi lozim?
+1-tizim bo'yicha ma'mur qo'llanmasi, 2-foydalanuvchi qo'llanmasi, 3- testlash va konstruktorlik hujjatlar
-1-tizim bo'yicha umumiy maílumotlar, 2-foydalanuvchilar maílumotlar, 3- tizim monitoringi va dasturlarni to'liq ma'lumotlariga
-1-tizim holatini tekshirish, 2-dasturlarni toíliq maílumotlariga
-1-tizimni baholash, 2-maímurni vazifalarini aniqlash
?
178.Tunnellash jarayoni qanday mantiqqa asoslangan?
+Konvertni kovertga joylash
-Konvertni shifrlash
-Bexato uzatish
-Konfidensiallik va yaxlitlik
?
179.Tunnellash mexanizmini amalga oshirilishda necha xil protokollardan foydalaniladi?
+3 ta
-4 ta
-6 ta
-7 ta
?
180.Umuman olganda, tashkilotning kompyuter muhiti qanday xavf- xatarga duchor boílishi mumkin?
+1-ma'lumotlarni yo'qotilishi yoki o'zgartirilishi, 2-Servisning to'xtatilishi
-1-maílumotlarni nusxalanishi, 2-virus hujumlari
-1-tarmoq hujumlari, 2-dastur xatoliklari
-1-foydalanuvchilarning maílumotlarini yoíqotilishi, 2-tizimni blokirovkalash mumkin
?
181.Umumiy tarmÓqni ikki qisimga ajratish va maílumotlar paketining chegaradan oítish shartlarini bajaradi-bu:
+TarmÓqlararÓ ekran
-XimÓyalanganlikni taxlillash vÓsitasi
-Hujumlarni aniqlash vÓsitasi (IDS)
-Antivirus dasturi
?
182.Umumiy holda himoyalash tadbirlari qaysi qism tizimnilarni o'z ichiga oladi?
+1-foydalanishni boshqarish, 2-ro'yxatga va hisobga olish, 3-kriptografiya, 4-yaxlitlikni ta'minlash
-1-tizimni boshqarish, 2-monitoring, 3-kriptografik
-1-foydalanishni ishdan chiqarish, 2-ro'yxatga va hisobga olish
-1-nusxalashni amalga oshirish, 2-ro'yxatga va hisobga olish, 3-hujumni aniqlash, 4-yaxlitlikni ta'minlash
?

183.Umumiy holda, himoyalash tadbirlari nechta qism tizimni o'z ichiga oladi?
+4 ta
-5 ta
-6 ta
-7 ta
?
184.Virtual himoyalangan tunnelning asosiy afzalligi-bu:
+Tashqi faol va passiv kuzatuvchilarning foydalanishi juda qiyinligi
-Tashqi faol va passiv kuzatuvchilarning foydalanishi juda oddiyligi
-Tashqi faol va passiv kuzatuvchilarning foydalanishi juda qulayligi
-Tashqi faol va passiv kuzatuvchilarning foydalanishi mumkin emasligi
?
185.Virtual ximoyalangan tunnelda qanday ulanish ishlatiladi?
+Ochiq tarmoq orqali oëtkazilgan ulanish
-Yuqori tezlikni ta¸minlovchi ulanish
-Himolyalangan tarmoq orqali oëtkazilgan ulanish
-Ekranlangan aloqa kanallarida oëtkazilgan ulanish
?
186.Virtual xususiy tarmoqda ochiq tarmoq orkali malumotlarni xavfsiz uzatishda nimalardan foydalaniladi?
+Inkapsulyasiyalash va tunnellashdan
-Tarmoqlararo ekranlardan
-Elektron raqamli imzolardan
-Identifikatsiya va autentifikatsiyadan
?
187.Virusga qarshi dasturlar zararlangan dasturlarning yuklama sektorining avtomatik nima qilishini taminlaydi?
+Tiklashni
-Ximoyalashni
-Ishlashni
-Buzulmaganligini
?
188.Viruslarni qanday asosiy alomatlar bo'yicha turkumlash mumkin?
+Yashash makoni, operatsion tizim, ishlash algoritmi xususiyati, destruktiv imkoniyatlari
-Destruktiv imkoniyatlari, yashash vaqti
-Tarmoq dasturlari tarkibini, aniqlashni murakkabligi boíyicha
-Dasturlarini va fayllarini yozilish algoritmi boíyicha, oíqilish ketma-ketligi boíyicha imkoniyatlari
?
189.Viruslarning hayot davri qanday asosiy bosqichlardan iborat?
+1-saqlanish 2-bajarilish
-1-yaratish 2-oíchirilish
-1-tarqalish 2-oízgartirilish
-1-koíchirilish 2-ishga tushirish
?
190.VPN konsepsiyasida ìvirtualî iborasi nima ma¸noni anglatadi?
+Ikkita uzel oërtasidagi ulanishni vaqtincha deb koërsatadi
-Ikkita uzel oërtasida ulanishni koërinmasligini ta¸kidlash
-Ikkita uzel oërtasidagi ulanishni optik tolaliligini ta¸kidlash
-Ikkita uzel oërtasidagi ulunishni doimiy deb koërsatish
?
191.Xar bir kanal uchun mustaqil ravishda maímotlar oqimini himoyalashni taíminlaydigan usulñbu:
+Kanalga moëljallangan himoyalash usullari
-Chekkalararo himoyalash usullari va uning tahlili
-Identifikatsiya usullari
-Maímurlash usullari
?
192.Xar bir xabarni maínbadan manzilgacha uzatishda umumiy himoyalashni taíminlaydigan usulñbu:
+Chekkalararo himoyalash usullari
-Kanalga moëljallangan himoyalash usullari
-Identifikatsiya usullari
-Autentifikatsiya usullari
?
193.Xarbiylar tomonidan kiritilgan axborot urushi atamasi maínosi nima?
+Qirgëinli va emiruvchi xarbiy harakatlarga bogëliq shafqatsiz va xavfli faoliyat
-Insonlarni xarbiy harakatlarga bogëliq qoërqituvchi faoliyat

-Xarbiy sohani kuch qudratiga bogëliq vayronkor faoliyat
-Xarbiy soha faoliyatini izdan chiqaruvchi harakatlarga bogëliq faoliyat bilan bog'langanligi
?
194.Xavfsizlik siyosatini madadlash qanday bosqich hisoblanadi?
+Eng muhim bosqich
-Ahamiyatsiz bosqich
-Moliyalangan bosqich
-Alternativ bosqich
?
195.Xavfsizlikga qanday yondoshish, toëgëri loyixalangan va yaxshi boshqariluvchi jarayon va vositalar yordamida xavfsizlik xavf-xatarlarini real vaqt rejimida nazoratlash, aniqlash va ularga reaksiya koërsatishga imkon beradi?
+Adaptiv
-Tezkor
-Alternativ
-Real
?
196.Xesh-funksiya algoritmlari qaysi javobda noto'g'ri ko'rsatilgan.
+DES, RSA
-Gammalash, sezar
-Kerberos
-FTP, TCP, IP
?
197.Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini koírsating?
+DDoS (Distributed Denial of Service) hujum
-Tarmoq hujumlari
-Dastur hujumlari asosidagi (Denial of Service) hujum
-Virus hujumlari
?
198.Yosh, koëpincha talaba yoki yuqori sinf oëquvchisi va unda oëylab qilingan xujum rejasi kamdan-kam axborot xavfsizligini buzuvchi odatdañbu:
+Sarguzasht qidiruvchilar
-Gëoyaviy xakerlar
-Xakerlar professionallar
-Ishonchsiz xodimlar
?
199.Yuklama viruslar tizim yuklanishida qanday vazifani bajaradi?
+Yuklanishida boshqarishni oluvchi dastur kodi
-Yuklanishida dasturlar bilan aloqani tiklash jarayoni
-Yuklanishida tizim xatoliklarini tekshirish
-Yuklanishida boshqarishni ishdan chiqarish
?
200.Zarar keltiruvchi dasturlar-bu:
+TrÓyan dasturlari, mantiqiy bÓmbalar
-Antivirus va makro dasturlar
-Ofis dasturlari va xizmatchi dasturlar
-Litsinziyasiz dasturlar
201.Zararli dasturlarni koírsating?
+Kompyuter viruslari va mantiqiy bombalar
-Letsinziyasiz dasturlar va qurilmalar turlari
-Tarmoq kartasi va dasturlar
-Internet tarmogíi dasturlari

?
202.Axborot xavfsizligini taíminlash tizimini yaratish jarayonida bajaruvchi burchlariga nimalar kirmaydi?
+Texnik vazifalar tuzish
-Tavakkalchilikni tahlil qilish
-Buzgíinchi xususiy modelini ishlab chiqish
-Axborotni chiqib ketish kanallarini aniqlash

?
203.Uyishtirilmagan tahdid, yaíni tizim yoki dasturdagi qurilmaning jismoniy xatoligi ñ buÖ

+Tasodifiy tahdid
-Uyishtirilgan tahdid
-Faol tahdid
-Passiv tahdid

?
204.Quyida keltirilganlardan qaysi biri xavfsizlikni taíminlash chora va tadbirlari sanalmaydi?
+Moliyaviy-iqtisodiy tadbirlar
-Qonuniy-huquqiy va odob-axloq meyorlari
-Tashkiliy tadbirlar
-Fizik va texnik himoya vositalari

?
205.Xavfsizlikni taíminlashning zamonaviy metodlari nimalarni oíz ichiga olmaydi?
+Sifat nazoratini
-Kritpografiyani
-Kirish nazoratini
-Boshqaruvni

?
206.Fizik va texnik himoyalash vositalarining funksiyasi nima?
+Tashkiliy meyorlar kamchiligini bartaraf etish
-Foydalanuchilarning tizim resurslariga kirish qoidalarini ishlab chiqish
-Kirishni cheklab qoíyish
-Yashirin holdagi buzgíinchilarni ushlab turuvchi omil

?
207.Himoyalangan tarmoqni loyihalash va qurish boíyicha toíliq yechimlar spektri oíz ichiga nimalarni olmaydi?
+Olingan maílumotlarning tahlili va hisobini
-Boshlangíich maílumotlarning aniq toíplamini
-Xavfsizlik siyosatini ishlab chiqishni
-Himoya tizimini loyihalashni

?
208.Maílumot uzatish tizimini qurish va uning ishlashi qaysi bitta asosiy printsip asosida amalga oshiriladi?
+Qonuniylik
-Qoíllaniladigan himoya vositalarining murakkabligi
-Texnik asoslanganligi
-Maxfiylik

?
209.Oíz vaqtida bajarish buÖ
+Axborot xavfsizligini taíminlash meyorlarining oldindan ogohlantiradigan xarakteri
-Meyorlarning doimiy mukammallashuvi
-Turli vositalarning muvofiqlashtirilgan holda qoíllanilishi
-Maílumot uzatish tizimi hayotiy siklining barcha bosqichlarida mos choralar qabul qilish

?
210.Nimalar axborot xavfsizligi siyosati doirasidagi maílumot uzatish tizimi tarmoqlarini himoya obyektlari emas?
+Foydalana olish, maílumot uzatish tizimida axborot xavfsizligini taíminlash tizimi
-Axborot resurslari, maílumot uzatish tizimida axborot xavfsizligini taíminlash tizimi
-Xabarlar
-Oddiylik va boshqarishning soddaligi, maílumot uzatish tizimi axborot xavfsizligini taíminlash tizimi

?
211.Maílumot uzatish tizimlarida tarmoqning axborot xavfsizligini taíminlash choralari qancha bosqichdan iborat?
+Uch
-Ikki
-Toírt
-Besh

?
212.Maílumot uzatish tizimlarida tarmoqning axborot xavfsizligini taíminlash choralarini amalga oshirishning uchinchi bosqichi nimani taxmin qiladi?
+Maílumot uzatish tizimlarida axborot xavfsizligini taíminlash tizimi arxitekturasini aniqlab beradi
-Maílumot uzatish tizimlarida axborot xavfsizligini taíminlash qoidalarini aniqlab beradi va uni urganib chiqadi
-Axborot xavfsizligini taíminlash vazifalarini aniqlab beradi
-Axborot xavfsizligining maílumotlar xisobini aniqlab beradi

?
213.Axborot xavfsizligini taíminlash tizimining egiluvchanligi deganda nima tushuniladi?
+Qabul qilingan va oírnatilgan himoya chora va vositalari
-Axborot xavfsizligini taíminlashga ketgan chiqimlar darajasining muvofiqligi
-Himoya vosita va choralarining doimiy mukammallashuvi
-Axborot xavfsizligini taíminlash

?
214.Uyishtirlgan tahdidni paydo boílishining bitta sababi nima?
+Maílumot uzatish tizimining himoyalanmaganligi
-Antiviruslar paydo boílishi va undan foydalanish usullari
-Foydalanuvchilarning savodsizligi
-Tasodifiy omillar

?
215.Quyidagi xalqaro tashkilotlardan qaysi biri tarmoq xavfsizligini taíminlash muammolari bilan shugíullanmaydi?
+BMT
-ISO
-ITU
-ETSI

?
216.Oëz DSt 15408 standarti qaysi standart asosida ishlab chiqilgan?
+ISO/IEC 15408:2005
-ISO/IEC 18028
-ISO/IEC 27001:1999y
-ISO 27002

?
217.Paydo boílish tabiatiga koíra barcha potentsial tahdidlar toíplamini qaysi ikkita sinfga ajratish mumkin?
+Tabiiy va suníiy
-Tasodifiy va uyishtirilgan
-Uyishtirilmagan va suníiy
-Tabiiy va notabiiy

?
218.Taísir etish xarakteriga koíra xavfsizlik tahdidlari nimalarga boílinadi?
+Faol va passiv
-Yashirin kanallardan foydalanish tahdidlari
-Butunlik va erkin foydalanishni buzish tahdidlari
-Ochiq kanallardan foydalanish tahdidlari

?
219.Amalga oshish ehtimoli boíyicha tahdidlar nimalarga boílinadi?
+Virtual
-Gipotetik
-Potentsial
-Haqiqiy

?
220.Har bir ATM paketi qancha baytdan iborat?
+53 bayt
-48 bayt
-32 bayt
-64 bayt

?
221.TCP/IP stekining bosh vazifasi nima?
+Paketli kichik tarmoqlarini shlyuz orqali tarmoqqa birlashtirish
-Uzatiladigan axborot sifatini nazorat qilish
-Maílumot uzatish tarmoqlarini birlashtirish
-Telekommunikatsiya liniyalari xavfsizligini taíminlash haqida birlashtirish

?
222.TCP/IP steki modelida qanday pogíonalar yoíq?
+Kanal, seans, taqdimot
-Tarmoqlararo, kanal, seans
-Tarmoq, taqdimot, transport
-Seans va tarmoq

?
223.IP texnologiyasining asosiy zaifligi nima?
+Ochiqlik va umumiy foydalana olishlik
-Yopiqlik
-Shifrlanganlik
-Foydalana olishlik va faqat bir kishi foydalanish

?
224.Qaysi protokolda IP-manzil tarmoq boíylab uzatish uchun fizik manziliga oízgartiriladi?
+ARP
-TCP/IP
-Frame Relay
-ATM

?
225.Axborot xavfsizligini taíminlovchi tizimni yaratishning qaysi bosqichida axborot xavfsizligi tahdidlari tasnif qilinadi?
+Taxdidklar tahlili
-Buzgíunchi xususiy modelini ishlab chiqish
-Axborot xavfsizligi tizimiga qoíyiladigan talablarni ishlab chiqish
-Obyektni oírganisgh

?
226.Asimmetrik shifrlash algoritmi nimaga asoslangan?
+Uzatuvchi qabul qiluvchining ochiq kalitidan foydalanadi, qabul qiluvchi esa xabarni ochish uchun shaxsiy kalitidan foydalanadi
-Uzatuvchi va qabul qiluvchi bitta kalitdan foydalanadi va undan qabul qiluvchi esa xabar nusxasini ochish uchun shaxsiy kalitidan foydalanadi
-Uzatuvchi va qabul qiluvchi uchta kalitdan foydalanadi
-Uzatuvchi ikkita kalit qabul qiluvchi bitta kalitdan foydalanadi

?
227.Simmetrik shifrlash algoritmiga nisbatan asimmetrik shifrlash algoritmining asosiy ustunligi nima?
+Kalitni uzatish uchun himoyalanmagan kanaldan foydalaniladi
-Kalitni uzatish uchun himoyalangan kanaldan foydalaniladi
-Kalitni uzatish uchun kombinatsiyali kanaldan foydalaniladi
-Kalitni uzatish uchun oddiy kanaldan foydalaniladi

?
228.Yuqori darajali chidamlilikni ta'minlash uchun RSA tizimi mualliflari qanday tarkibdagi sonlardan foydalanishni tavsiya etishadi?
+Taxminan 200 ta o'nlik raqamli sonlar
-Taxminan 2000 ta o'nlik raqamli sonlar
-Taxminan 20 ta o'nlik raqamli sonlar
-Taxminan 15 ta o'nlik raqamli sonlar

?
229.Qanday tarzda ochiq kalitli kriptotizim algoritmlaridan qo'llaniladi?
+Uzatiladigan va saqlanadigan ma'lumotni mustaqil himoyalash vositasi sifatida
-Foydalanuvchilarni identifikatsiya qilish vositasi sifatida va himoyalash vositasi sifatida
-Kalitlarni taqsimlash vositasi sifatida
-Foydalanuvchilarni autentifikatsiya qilish vositasi sifatida

?
230.Simmetrik shifrga nisbatan asimmmetrik shifrning ustunligi nima?
+Maxfiy shifrlash kaliti faqat bir tomonga ma'lum bo'lishi
-Ishonchli kanal bo'ylab maxfiy kalitni oldindan uzatish shart emasligi
-Katta tarmoqlardagi simmetrik kriptotizim kalitlari asimmetrik kriptotizimga nisbatan ancha kam
-Katta tarmoqlardagi asimmetrik kriptotizim kalitlari simmetrik kriptotizimga nisbatan ancha kam

?
231.Qanday turdagi blokli shifrlar mavjud?
+O'rnini almashtirish shifri va almashtirish (qaytadan qo'yish) shifrlari
-Almashtirish shifrlari
-O'rnini almashtirish shifrlari va almashtirish (qaytadan qo'yish) deshifrlari
-Qaytadan qo'yish shifrlari

?
232.Ochiq kalitli kriptografiya metod va g'oyalarini tushunish nimada yordam beradi?
+Kompyuterda parol saqlashga
-Seyfda parol saqlashga
-Qutida parol saqlashga
-Bankda parol saqlashga

?
233.Kriptotizimlar qaysi qaysi ikki guruhga bo'ladi?
+1-Simmetrik (bir kalit), 2-Asimmetrik (ikki kalit)
-1-O'rnini o'zgartirish, 2-Kalitlarni taqsimlash (ikki kalit)
-1-Gamma metodi, 2-kalit almashish
-1-Tarmoq bo'ylab shifrlash, 2-Kalitlarni taqsimlash

?
234.OSI modelining qaysi pogíonasida kirishni nazorat qilinmaydi?
+Taqdimot
-Tarmoq
-Kanal
-Sens satxi

?
235.Tashkiliy chora tadbirlarga nimalar kiradi?
+Davlat yoki jamiyatda shakllangan aníanaviy odob-axloq meyorlari
-Rekvizitlarni taqsimlash, foydalana olishni cheklash
-Foydanalanuvchining tizim resurslaridan foydalana olish qoidalarini ishlab chiqish tadbirlari
-MOBT vositalari

?
236.Identifikatsiya ñ buÖ
+Tizim elementini tanib olish jarayoni, bu jarayon identifikator tomonidan amalga oshiriladi
-Foydalanuvchi jarayonini identifikatsiyalashning haqiqiyligini aniqlash va ular tomonidan amalga oshiriladi
-Joriy ma'lumotlar massivi vaqt oraligíida oízgarmaganligini tasdiqlash
-Tarmoq foydalanuvchisining haqiqiyligini o'rnatish

?
237.Autentifikatsiya ñ buÖ
+Foydalanuvchi jarayoni, qurilmasi yoki boshqa kompanentlarni identifikatsiyalashning haqiqiyligini aniqlash
-Tizim elementini tanib olish jarayoni, bu jarayon identifikator tomonidan amalga oshiriladi va autentifikatsiyalashning haqiqiyligini aniqlash
-Joriy ma'lumotlar massivi vaqt oraligíida oízgarmaganligini tasdiqlash
-Tarmoq foydalanuvchisining haqiqiyligini o'rnatish

?
238.Tarmoq foydalanuvchisini autentifikatsiya qilish ñ buÖ
+Tarmoq foydalanuvchisining haqiqiyligini o'rnatish
-Joriy tarmoq haqiqiyligini o'rnatish
-Joriy ma'lumotlar massivi vaqt oraligíida oízgarmaganligini tasdiqlash
-Aloqa kanallaridan olingan ma'lumot haqiqiyligini o'rnatish

?
239.Tarmoq autentifikatsiyasi ñ buÖ
+Kirish ruxsati olingan joriy tarmoq haqiqiyligini o'rnatish
-Joriy ma'lumotlar massivi vaqt oraligíida oízgarmaganligini tasdiqlash
-Aloqa kanallaridan olingan ma'lumot haqiqiyligini o'rnatish
-Himoyalangan axborotga ega bo'lish uchun ruxsat talab etiladigan

?
240.Parol ñ bu Ö
+Tizim yoki fayllarga kirish ruxsatini olish uchun qo'llaniladigan kod
-Tizimga kirish dasturi
-Tarmoq elementlarining belgilanishi va ularni xotirada saqlab qolish jarayoni
-Shifrlangan simvollar to'plami

?
241.Elektron imzo ñ buÖ
+Boshlang'ich ma'lumotlarga bir tomonlama o'zgartirish funksiyasini qo'llash yoíli bilan olingan baytlar toíplami
-Foydalanuvchini tarmoq resurslariga murajaatidagi autentifikatsiya vositasi va uni qo'llash yoíli bilan olingan baytlar toíplami
-Asimmetrik kalitlar juftligi egasining haqiqiyligini aniqlash vositasi
-Parolli himoyaga ega tizim yoki fayllarga kirish ruxsatini olish uchun qo'llaniladigan kod

?
242.Sertifikat ñ buÖ
+Foydalanuvchini tarmoq resurslariga murajaatidagi autentifikatsiya vositasi
-Asimmetrik kalitlar juftligi egasining haqiqiyligini aniqlash vositasi
-Parolli himoyaga ega tizim yoki fayllarga kirish ruxsatini olish uchun qo'llaniladigan kod
-Boshlang'ich ma'lumotlarga bir tomonlama o'zgartirish funksiyasini qo'llash yoíli bilan olingan baytlar toíplami

?
243.Ochiq kalit sertifikati ñ buÖ
+Asimmetrik kalitlar juftligi egasining haqiqiyligini aniqlash vositasi
-Parolli himoya samaradorligi parollarning sir saqlanish darajasiga bog'liq
-Boshlang'ich ma'lumotlarga bir tomonlama o'zgartirish funksiyasini qo'llash yoíli bilan olingan baytlar toíplami
-Foydalanuvchini tarmoq resurslariga murajaatidagi autentifikatsiya vositasi

?
244.Frame Relay ñ buÖ
+OSI tarmoq modelining kanal pogíona protokoli
-Parolli himoyaga ega tizim yoki fayllarga kirish ruxsatini olish uchun qo'llaniladigan kod
-Boshlang'ich ma'lumotlarga bir tomonlama o'zgartirish funksiyasini qo'llash yoíli bilan olingan baytlar toíplami
-Foydalanuvchini tarmoq resurslariga murajaatidagi autentifikatsiya vositasi

?
245.Noqonuniy kirish tahdidlari nima bilan bog'liq?
+Ma'lumot maydoni va protokolli bloklarining uzatiladigan boshqaruvchi sarlavhalaridagi axborot tarkibini tahlil qilish imkoni bilan
-Maílumotlar protokolli bloklarining tarmoq boíylab uzatiladigan axborot tarkibi oízgarishi bilan
-MUT mijoziga xizmat ko'rsatish normal darajasining yoíqolishi yoki buzg'inchi harakati natijasida resursga kirish toíliq cheklanib qolish ehtimolligi bilan
-Ma'lumotlar kadrining sarlavha maydonlarini noqonuniy o'zgartirish yoíli bilan xabar uzatish tezligini kamaytirish

?
246.Butunlik tahdidlari nima bilan bog'liq?
+Maílumotlar protokolli bloklarining tarmoq boíylab uzatiladigan axborot tarkibi oízgarishi bilan
-MUT mijoziga xizmat ko'rsatish normal darajasining yoíqolishi yoki buzg'inchi harakati natijasida resursga kirish toíliq cheklanib qolish ehtimolligi bilan
-Protokolli bloklar boshqaruv sarlavhalarini va ma'lumot maydonlarining axborot tarkibini tahlil qilish imkoniyati bilan
-Ma'lumotlar kadrining sarlavha maydonlarini noqonuniy o'zgartirish yoíli bilan xabar uzatish tezligini kamaytirish

?
247.Funktsionallik tahdidlari nima bilan bog'liq?
+MUT mijoziga xizmat ko'rsatish normal darajasining yoíqolishi yoki buzg'inchi harakati natijasida resursga kirish toíliq cheklanib qolish ehtimolligi bilan
-Protokolli bloklar boshqaruv sarlavhalarini va ma'lumot maydonlarining axborot tarkibini tahlil qilish imkoniyati bilan
-Maílumotlar protokolli bloklarining tarmoq boíylab uzatiladigan axborot tarkibi oízgarishi bilan
-Ma'lumotlar kadrining sarlavha maydonlarini noqonuniy o'zgartirish yoíli bilan xabar uzatish tezligini kamaytirish

?
248.Frame Relay texnologiyasining zaif jihatlari nima?
+Xabar uzatishni ma'lumotlar kadrini o'chirish yoki buzish yo'li bilan cheklab qo'yish
-Xabar uzatish tezligini kamaytirish
-Ma'lumotlar kadrining sarlavha maydonlarini noqonuniy o'zgartirish va buzish yo'li bilan cheklab qo'yish
-Garovni faollashtirish ehtimoli

?
249.ATM tarmoqlarinig xavfsizligiga tahdid deganda nima tushuniladi?
+Ma'lumot uzatish tizimlari axborot sohasiga boílgan ehtimolli taísir
-Protokolli bloklarning boshqaruv sarlavhalari va ma'lumot maydonlarini axborot tahlili qilish ehtimolligi
-Ma'lumotlar protokolli bloklarining axborot tarkibini o'zgartirish
-Buzg'inchi harakati natijasida mijozga xizmat ko'rsatish normal darajasining yoíqolishi ehtimolligi

?
250.Axborot va uni tashuvchisining noqonuniy tanishtirsh yoki xujjatlashni bartaraf etgan holdagi holatini qanday termin bilan atash mumkin?
+Konfidentsiallik
-Butunlik
-Foydalana olishlilik
-Zaiflik
?
251.Axborotning noqonuniy buzilishi, yo'qolishi va o'zgartirilishi bartaraf etilgan holati qanday ataladi?
+Axborot butunligi
-Axborot xavfsizligiga tahdidlar

-Axborot xavfsizligi
-Axborot sifati

?
252.Ochiq autentifikatsiya ñ bu Ö
+Erkin (nol) autentifikatsiyali algoritm
-Mijoz punkti va kirish nuqtasi WEP ni qo'llab-quvvatlashi va bir xil WEP-kalitlarga ega bo'lishi kerak
-Ochiq matnli chaqiruv freymi bilan javob beruvchi kirish nuqtasi
-Autentifikatsiya algoritmining qo'llanilishini ko'rsatuvchi signal

?
253.Niyati buzuq inson tomonidan tarmoq bo'ylab uzatilayotgan axborotni himoya tizimining zaif nuqtalarini aniqlash maqsadida ushlab olish nima deb ataladi?
+Eshitish
-Spam tarqatish
-Zaiflik
-Foydalana olishlilik

?
254.Foydalanuvchi sohasining xavfsizligiÖ
+Xavfsizlik darajasi yoki xavfsizlikni taíminlash metodlarini amalgam oshirishga doir maílumotni foydalanuvchiga taqdim etish
-Maílumotlar konfidentsialligi (mobil stantsiya oírtasidagi shifr kaliti va algoritm boíyicha rozilik)
-Ro'yxat paytida, abonentlar pul to'lamasdan xizmatlardan foydalangandagi frod (qalloblik)
-Mobil qurilmaning xalqaro identifikatsion raqami IMEI ni identifikatsiyalash va ma'lumotlar butunligini amalgam oshirishga doir maílumotni foydalanuvchiga taqdim etish

?
255.3G tarmogíida xavfsizlik tahdidlari nima?
+Niqoblanish, ushlab olish, frod (qalloblik)
-Niqoblanish, ushlab olish, butunlik
-ushlab olish, frod (qalloblik), foydalana olishlik
-Frod (qalloblik), niqoblanish

?
256.LTE xavfsizlik tizimiga talablar nima?
+Ierarxik asosiy infratuzilma, xavfsizlikning oldini olish kontsepsiyasi, LTE tarmoqlari oírtasida maílumot almashinuvi uchun xavfsizlik mexanizmlarini qoíshish
-3G tizim xizmatlar xavfsizligi va uning butunligi, shaxsiy maílumotlarni himoyalash va tarmoqlari oírtasida maílumot almashinuvi uchun xavfsizlik mexanizmlarini qoíshish
-Xavfsizlikning oldini olish kontsepsiyasi
-2G tarmoqlari oírtasida maílumotlar almashinuvi uchun xavfsizlik mexanizmlarini qoíshish

?
257.Tarmoqlararo ekranlarga qoíyilgan funksional talablar qanday talablarni oíz ichiga oladi?
+Tarmoq va amaliy pogíonada filtrlash, tarmoq autentifikatsiyasi vositalariga talablarni
-Transport va amaliy pogíonada filtrlash
-Faqat transport pogíonasida filtrlash
-Tarmoq autentifikatsiya vositalarga talablar va faqat transport pogíonasida filtrlashjarayoni

?
258.Amaliy pogíona shlyuzlari nima?
+Amaliy pogíonadagi barcha kiruvchi va chiquvchi IP-paketlarni filtrlaydi va ilovalar shlyuzi uni toíxtatib soíralyotgan xizmatni bajarish uchun tegishli ilovani chaqiradi
-Taqdimot haqida tushayotgan har bir soírovga javoban tashqi tarmoq seansini tashkillashtiradi

-IP paketni aniq foydalanuvchi qoidalariga mavjudligini tekshiradi va paketning tarmoq ichiga kirish huquqi borligini aniqlaydi
-3G va LTE tarmoqlari oírtasida maílumotlar almashinuvi uchun xavfsizlik mexanizmlarini qoíshish

?
259.Tarmoqlararo ekran qanday himoya turlarini taímilaydi?
+Nomaqbul trafikni cheklab qoíyish, kiruvchi trafikni ichki tizimlarga yoínaltirish, tizim nomi kabi maílumotlarni berkitish, tarmoq topologiyasi
-Nomaqbul trafikni cheklab qoíyish, kiruvchi trafikni faqat moíljallangan tashqi tizimlarga yoínaltirish
-Kiruvchi trafikni faqat moíljallangan tashqi tizimlarga yoínaltirish
-Tizim nomi kabi maílumotlarni berkitish, tarmoq topologiyasi, tarmoq qurilmalari turlari va foydalanuvchilar identifikatorlarini qiyosiy tahlillari

?
260.Tarmoqlararo ekran qurishda hal qilinishi kerak boílgan muammolar nimalarni taíminlaydi?
+Ichki tarmoq xavfsizligi, aloqa seanslari va tashqi ulanish ustidan toíliq nazorat qilish, xavfsizlik siyosatini amalgam oshirishning kuchli va egiluvchan boshqaruv vositalari
-Tashqi tarmoq xavfsizligi, aloqa seanslari va ichki ulanish ustidan toíliq nazorat qilish va ularning xavfsizlik siyosatini amalgam oshirishning kuchli va egiluvchan boshqaruv vositalari
-Tarmoq tuzilishi oízgrarganda tizimni kuchli rekonfiguratsiya qilishni taímilaydi
-Ichki tarmoq xavfsizligi, aloqa seanslari va tashqi ulanish ustidan toíliq nazorat qilish

?
261VPN qanday avzalliklarga ega?
+Axborot sir saqlanadi, masofaviy saytlar axborot almashinuvini tez amalga oshirishadi
-Axborot xavfsizligini taíminlash tizimining ruxsat etilmagan har qanday harakatlardan ishonchli himoyalash
-Tarmoqlararo ekran boshqarish tizimining yagona xavfsizlik siyosatini markazlashtirilgan tarzda olib borish
-Tashqi ulanishlar orqali foydalanuvchilarning kirishini avtorizatsiyalash

?
262.VPN qanday qismlardan tashkil topgan?
+Ichki va tashqi tarmoq
-Masofaviy va transport tarmogíi
-Himoyalangan va ishonchli tarmoq
-Intranet VPN va Extranet VPN

?
263.VPN qanday xarakteristikalarga ega?
+Trafikni eshitishdan himoyalash uchun shifrlanadi va VPN koíp protokollarni qoíllab-quvvatlaydi
-Axborot sir saqlanadi, masofaviy saytlar axborot almashinuvini tez amalga oshirishadi va urganib chiqadi
-VPN koíp protokollarni qoíllab-quvvatlamaydi
-Ulanish faqat uchta aniq abonent oírtasidagi aloqani taíminlaydi

?
264.Axborot xavfsizligi qanday asosiy xarakteristikalarga ega?
+Butunlik, konfidentsiallik, foydalana olishlik
-Butunlik, himoya, ishonchlilikni urganib chiqishlilik
-Konfidentsiallik, foydalana olishlik
-Himoyalanganlik, ishonchlilik, butunlik

?
265.Maílumotlarni uzatish tarmogíining axborot xavsizligini taíminlash bosqichlari nimalarni oíz ichiga oladi?
+Obyektlarning umumiy xarakteristikasi, xavfsizlikka tahdidlar tahlili va ularni amalga oshirish yoíllarini
-Foydalana olishlik, yaíni resurslarni ruxsat etilmagan cheklab qoíyishdan himoya qilish va ularni amalga oshirish
-Trafikni eshitishmasliklari uchun shiflab himoya qilinadi
-Butunlik, yaíni axborotni ruxsatsiz buzilishidan himoya qilish

?
266.NGN turli kichik tizimlarining xavfsizligiga qoíyiladigan talablar toíplami nimalarni oíz ichiga oladi?
+Xavfsizlik siyosati, sirlilik, kafolat, kalitlarni boshqarish
-Butunlik, konfidentsiallik, foydalana olishlik
-Butunlik, identifikatsiya va xavfsiz roíyxatdan oítish
-Autentifikatsiya, avtorizatsiya, kirishni boshqarish, konfidentsiallik

?
267.NGN tarmogíi operatoriga boílgan tahdidlar nechta qismdan iborat?
+4
-3
-2
-5

?
268.NGN tarmogíiga oítishda paydo boíladigan xavfsizlik tahdid turi va manbalari nimalar?
+UfTT tahdidlari ñ telefon tarmogíi xizmatlari operatorining aníanaviy tahdidlari, Internet tarmogíi tahdidlari, IP-tahdidlar
-UfTT tahdidlari ñ telefon tarmogíi xizmatlari operatorining aníanaviy tahdidlari
-Internet tarmogíi tahdidlari ñ internet-xizmati yetkazib beruvchilarining noaníanaviy tahdidlari va tarmoqda Internet tarmogíi tahdidlari, IP-tahdidlar
-IP texnologiyasining umumiy zaifliklari bilan bogíliq boílgan DNS ñ tahdidlar

?
269.Axborot xavfsizligining obyektlari nimalar?
+Liniya-kabel inshootlari, axborot resurslari
-Aloqa tarmogíi foydalanuvchilari va axborot resurslari
-Aloqa operatori xodimi va liniya-kabel inshootlari
-Aloqa operatori xodimi va boshqa shaxslar

?
270.Axborot xavfsizligining subyektlari nimalar?
+Aloqa tarmogíi foydalanuvchilari, aloqa operatori xodimi va boshqa shaxslar
-Axborot xavfsizligini taíminlash vositalari va liniya-kabel inshootlari va binolar
-Boshqaruv tizimi qurilmasi va taktli sinxronizatsiya tizimi qurilmasi
-Liniya-kabel inshootlari va axborot resurslari

?
271.IP-telefoniya va multimediali aloqa muhitida xavfsizlikni taíminlash qanday amalga oshiriladi?
+Foydalanuvchi, terminal va server autentifikatsiyasi, chaqiruvni avtorizatsiyalash
-Faqat terminalni autentifikatsiyalash: VoIP xizmatini yetkazib beruvchilar ularning xizmatidan kim foydalanishini bilishlari shart
-Faqat terminalni identifikatsiyalash: VoIP xizmatini yetkazib beruvchilar ularning serverlaridan kim foydalanishini bilishlari shart
-Chaqiruvni va serverni avtorizatsiyalash, autentifikatsiyalash

?
272.Turli shifrlash tizimlarini ishlan chiqqanda va ulardan foydalangan qanday omil asosiy hisoblanadi?
+Xabardagi maílumotlar sirlilik darajasi
-Shifrlash tizimining qiymati
-Shifrlash tizimini qoíllash muhiti
-Electron imzoni amalgam oshirishbi nazorati

?
273.Simmetrik shifrlashning mazmuni nima ñ ikki marta oírniga qoíyish?
+Ikkinchi jadval hajmi shunday tanlansinki, uning ustun va satr uzunligi birinchi jadvalga nisbatan boshqacha boílsin
-Ikkinchi jadval hajmi shunday tanlansinki, uning satr uzunligi birinchi jadvaldagidek bir xil, ustun uzunligi esa boshqacha boílsin
-Ikkinchi jadval hajmi shunday tanlansinki, uning ustun va satr uzunligi birinchi jadval bilan bir xil boílsin

-Ikkinchi jadval hajmi shunday tanlansinki, uning satr uzunligi birinchi jadvaldagidek bir xil emas, ustun uzunligi esa boshqacha boílsin

?
274.Axborot xavfsizligining asosiy vazifalari?
+Maílumotlar uzatishning butunligi va konfidentsialligini ximoya qilish, maxsus ishlarni olib borish butunlikni va konfidentsiallikni ximoya qilish, kiruvchanlikni taminlash
-Maílumotlar uzatishda maxsus ishlarni olib borish
-Maílumotlar uzatishda maxsus ishlarni olib boorish va va konfidentsialligini ximoya qilish, maxsus ishlarni olib borish butunlikni va konfidentsiallikni ta'minlash asosida taxlillar
-kiruvchanlikni taminlash

?
275.Abonent foydalanuvchilari servislarga ruxsatsiz kirish bu...
+Bu xar qanday faoliyat,oxirgi foydalanuvchi xavsizlikning etarli darajasiz IPTV xizmatiga ega boladi, oíz navbatida paketdagi kanallar sonini koípaytiradi, shuningdek VoD xizmatini taqdim qiladi
-Uzatilayotgan trafigda kiritilgan oízgartirishlar va ruxsatsiz kirishning bazi misollarini oíz ichiga oladi
-Buzgíunchi shaxsiy maílumotlar saqlanadigan maílumotlar ombori servisiga kirishga ruxsat olishi mumkun
-Markaziy stansiya unsurlari ustidan boshqarishni taminlash uchun Middleware- servisini ishlatishni taminlaydi va konfidentsialligini ximoya qilish, maxsus ishlarni olib borish butunlikni va konfidentsiallikni

?
276.ìYevropa mezonlariî axborot xavfsizligini tashkil qiluvchi quidagilarini koírib chiqadi?
+Identifikatsiya va autentifikatsiya, kirishni boshqarish
-Xavsizlikning vazifalar spetsifikatsiyasi
-Kiruvchanli, axboropt aniqligi
-Axborot aniqligi, obektlardan qayta foydalanish va ularni nazoratlash

?
277.Mezonlarni xavsizlik vazifalari spetsifikatsiyalarida ajratishni tavsiya qilish?
+Identifikatsiya va autentifikatsiya, kirishni boshqarish
-Xavsizlikning vazifalar spetsifikatsiyasi
-Kiruvchanli, axboropt aniqligi
-Axborot aniqligi, obektlardan qayta foydalanishni tahlillarini nazoratlash

?
278.Aloqa kanlidagi xatolarni qanday koírinishdagi ikki turga ajratish mimkin
+Additiv va multiplikativ
-Pozitiv va negativ
-Inkrement va dekrement
-Qoniqarli va qoniqarsiz

?
279.Autentifikatsiya qobiliyatini tanlash boíyicha qanday faktor hisobga olinadi?
+Obíyektga kirish huquqini subíyektga taqdim etish
-Autentifikatsiyani apparat-dasturini taíminlash narxi
-Tizimlar maqsadga muvofiqligi
-Axborot qiymati

?
280.Autentifikatsiyani keng tarqalgan sxema turi?
+Bir martalik parollarni qoíllanishi
-Biometrik tavsiflarni qoíllanishi
-Koíp martalik parollarni qoíllanishi mezonlari
-Xabar muallifi savolini yechish

?
281.Parol VA/YOKI login xato kiritilgan boílsa tizim nima xaqida xabar beradi
+Kirishni avtorizatsiyalash imkoniyati yoíqligi
-Autentifikatsiyani toígíriligi to'g'risida xabar berilishi
-Autentifikatsiyani xatoligi
-Xaqiqiylikni tasdiqlash

?
282.Sertifikatsiyaga asoslangan autentifikatsiya usuli nimalarga asoslangan?
+Axborot tashuvchilar
-Tarmoq protokollari va tarmoq testerlari
-Interfeyslar, portlar, tizimlar
-Apparatura va vosita tizimlari orasidagi telekommunikatsiya liniyasiga

?
283.Xatolik tufayli, bilib yoki bilmay, yoki qasdan ruxsat etilmagan kirishni amalga oshirgan shaxs ñ bu Ö
+Yovuz niyatli odam
-Tizim administratori
-Yuridik shaxs
-Buzgíunchi

?
284.Parol tanlashga qanday talablar qoíyiladi?
+Parol ochish uchun qiyin boílishi lozim, noyob va oson xotirada qolishi kerak
-Parol oddiy va qisqa boílishi kerak
-Parol doimiy va oson xotirada qolishi kerak hech kimda bulmaga va oson xotirada qolishi kerak
-Parol koíp simvolli va uzun bolishi kerak

?
285.Qaysi texnologiya yordamida tezligi 75 Mb/s ni, maksimal oraliq 10 km boílgan simsiz kirish imkoniyatini beradi?
+Wi-Max
-Wi-Fi
-LTE (yangi avlodi)
-4G

?
286.Shifrlarni almashtirish qanday guruxlarga boílinadi?
+Monoalfavitli (Tsezar kodi) , polualfavitli (Vijiner shifri, Djeffersjy tsilindri)
-Monoalfavitli, Tsezar kodi
-Vijiner shifri, Djeffersjy tsilindri polualfavitli bulmagan (deffi helman shifri, Djeffersjy tsilindri)
-Polualfavitli

?
287.Shifrlash algoritmlarida koírib oítilgan yolgíon maílumotlarga bogílanishdan himoyalash nima deb ataladi?
+Imitovstavkalarni ishlab chiqarish
-Reflektiv
-Immunitet
-Maxfiy kalit ishlab chiqarish algoritmlari

?
288.Simsiz tarmoqlar uchun nechta taxdidlar mavjud?
+3
-2
-5
-6

?
289.Xeshlash bu:
+Kodlash
-Siqish
-Dekodkash

-Kengaytirish

?
290.ERIni qurishda qanday kaitdan foydalaniladi?
+Ochiq va maxfiy
-Maxfiy va maxfiy emas
-Ochiq va yopiq
-Maxfiy va yopiq

?
291.Tasodifiy taxdidlarning paydo boílish sabablariga quyida keltirilganlardan qaysilari kirmaydi:
+Viruslar, yashirish
-Rad etish va qurilmalarning toíxtab qolishlari
-Telekommunikatsiya liniyalaridagi xatolar va shovqinlar
-Strukturali, algoritmik va dasturiy xatolar

?
292.Xavfsizlikka taxdidlarni shartli ravishda qanday ikki guruxga boílish mumkin?
+Tasodifiy va oldindan moíljallangan
-Strukturali va algoritmik ishlab chiqishga moíljallangan
-Sxemali va texnik-tizimli
-Oldindan moíljallangan

?
293.Tizim obíektlariga nisbatan amalgam oshiriladigan boílishi mumkin boílgan taxdid tushunchasi ostida nima tushuniladi?
+Zaiflik
-Butunlik
-Axborot ximoyasi
-Autentifikatsiya

?
294.Maílumotlarni etkazib berishni rad etishlardan himoyalash xizmati oízaro ochiq tizimlarning etalon modeli qaysi pogíonaga tegishli?
+Amaliy
-Tarmoq
-Seans
-“ransport

?
295.Kirish nazorati quyidagi operarsiyalar yordamida taíminlanishi mumkinÖ
+Identifikatsiya va Autentifikatsiya
-¿vtorizatsiya va verifikatsiya (tahlillari)
-Shifrlash va deshifrlash
- riptografik algoritmlar

?
296.Avtorizatsiya nima?
+Obíektga kirish huquqini subíektga taqdim etish
-Foydalanuvchi, uskuna yoki komyuter tizimlari indentifikatsiyasi haqiqiyligini tekshirish
-Avvaldan belgilangan bir yoki bir necha identifikatorlar yordami bilan tizim elementlarini aniqlash jarayoni
-Tarmoqga ulanishni oírnatish

?

297.Identifikator nimani ifodalaydi?
+Noyob nomer
-Dasturli tizim
-Kirish uchun parol
-Dastur-utilit

?
298.Subíyekt ostiga kirishni boshqarish mexanizmi deganda nima tushuniladi?
+Foydalanuvchi
-Texnik resurslar
-Tarmoq
-Administrator

?
299.Zaiflik qanday boíladi?
+Uyushtirilgan
-Subyektiv
-Obyektiv
-Konfidentsiallikni ta'minlash

?
300.Maílumotlarni uzatishda sir saqlashni taminlab beradigan mexanizm qaysi?
+Shiflash mexanizmi
-Kirishni boshqaruvchi mexanizm
-Trafikni ximoya qilish mexanizmi
-Audentefikatsiyani taminlash mexanizmi
301.Xavfsizlikka tahdid qaysi 2 ta sinfga bolinadi?
+Uyushtirilgan va Tasodifiy tahdid
-Oldindan oíylangan va oldindan oíylanmagan tahdid
-Uyushtirilmagan va uyushtirilgan tahdid
-Uyushtirilgan va Tasodifiy tahdid

?
302.Keltirilganlardan qaysi biri tasodifiy tahdid sabablariga taalluqli emas?
+Buzgíunchilar yaratgan tahdid
-Qurilmani ishdan chiqishi va rad qilishi
-Telekommunikatsiya liniyalaridagi xatolik va qarshiliklar
-Foydalanuvchilar va xodimlar xatolari

?
303.Axborot xavfsizligining asosiy xarakteristirflari nimalar?
+Konfidentsiallik, butunlik, foydalana olishlik
-Konfidentsiallik, aniqlik
-Sirlilik, butunlik, foydalana olishlikni urganib chiqish
-Identifikatsiya va autentifikatsiya

?
304.Tarmoq xavfsizligini taíminlash uchun hal qilinishi kerak boílgan muhim vazifalardan biri nima?
+Taqdim etiladigan xizmatlarga foydalanuvchilarning noqonuniy kirishdan tarmoqni ximoya qilish
-Tarmoqni qizib ketishidan himoya qilish
-Tarmoqni litsensiyalangan dasturlarni faollashtirilishidan himoya qilish va noqonuniy kirishdan tarmoqni ximoya qilish
-Tarmoqni mexanik buzilishlardan himoya qilish

?
305.ìKonfidentsiallikî deganda nimani tushunasiz?
+Axborotga noqonuniy ega boílishdan himoya
-Axborotni noqonuniy buzishdan himoya
-Axborot va resurslarni noqonuniy cheklab qoíyishdan himoya

-Resurslardan noqonuniy foydalanishdan himoya

?
306.Axborot oqimlarini tahlil qilishdan himoyalovchi mehanizm nima?
+Trafikni himoyalash mehanizmi
-Kirishni nazorat mehanizmi
-Marshrutizatsiyani boshqarish mehanizmi
-Autentifikatsiyani taíminlash mehanizmi

?
307.Qanday obyektlarni telekommunikatsiya tarmoqlarida tarmoq xavfsizligining asosiy obyektlariga kiritish mumkin emas?
+Marshrutizatorlar va routerlar
-Information resurslar
-Abonentlar kirish tugunlari
-Telekommunikatsiya liniyalari, dasturiy taíminot

?
308.Qaysi standartda NGN asosiy tarmogíining xavfsizlik jihatlarini koíriladi?
+ETSI TS 187 003 VI. 1.1 (02/2008)
-X.1051
-ISO/IEC 27006:2007 07 VI. 2.1 (10/2002)
-ISO/IEC 27005:2007

?
309.ISO/IEC 18028 standarti nechta qismdan iborat?
+Beshta
-Uchta
-Oltita
-Ikkita

?
310.X.25 texnologiyasining xizmat qismida paket formati qancha bayt boíladi?
+6-9 bayt
-7-8 bayt
-10 bayt
-9-10 bayt

?
311.Frame Relay texnologiyasining aniq taírifini qaysi javobda keltirilgan?
+OSI tarmoq modelining kanal pogíona protokoli
-OSI modelining tarmoq pogíona protokoli tahlili
-Seans pogíona protokoli
-Transport pogíona protokoli

?
312.Tarmoq trafigi tahlili vositasida hujumlardan himoyalanishning yagona vositasi nima?
+Kriptoprotokollardan foydanalanish
-Axborotning maxfiyligi
-Cheklov qoíyish
-Antiviruslardan foydalanishning imkoniyatlari

?
313.Internet tarmogíida uzatiladigan paket qancha qismdan iborat?
+Maílumotlar maydoni va sarlavhadan
-Steklardan
-Maílumotlar maydoni va kichik sarlavhadan
-Maílumotlar satri va yacheykasidan

?

314.Simsiz aloqa tarmoqlari axborot xavfsizligining asosiy qismlari nima?
+Konfidentsiallik, butunlik, foydalana olishlik
-Butunlik, ishonchlilik, tahlil
-Himoyalanganlik, kafolatlanganlik
-Ishonchlilik, himoyalanganlik va kafolatlanganlik

?
315.Simsiz tarmoqlar uchun nechta asosiy tahdidlar mavjud?
+3
-2
-5
-6

?
316.Axborot xavfsizligining zaifligi qanday boílishi mumkin?
+Obyektiv, subyektiv, tasodifiy
-Konfidentsiallik, butunlik, foydalana olishlik
-Ishonchlilik va kafolatlanganlik
-Subyektiv, tasodifiy, himoyalangan

?
317.Gogen Meziger modeli nimaga asoslangan?
+Avtomatlar nazariyasiga
-Resurslar nazariyasiga
-Nisbiylik nazariyasiga
-Ehtimollar nazariyasiga

?
318.Wi-MaX axborot xavfsizligining subyektlari keltirilgan javobni tanlang?
+Simsiz tarmoq foydalanuvchilari, operator xodimlar va boshqa shaxslar
-Guruh administratorlari, mashina muhandislari
-Operator xodimlar, axborot xavfsizligini taíminlash vositalarining tahlili
-Axborot resurslari, boshqaruv tizimi qurilmasi

?
319.Tahdidlarning 80 % - bu Ö
+Tashqi tahdidlar
-Ichki va tashqi tahdidlar
-Fizik tahdidlar
-Ichki tahdidlar

?
320.Simmetrik shifrlash algoritmlari (yoki maxfiy kalitli kriptografiya) nimaga asoslangan?
+Uzatuvchi va qabul qiluvchi bitta kalitdan foydalanadi
-Uzatuvchi va qabul qiluvchi turli kalitlardan foydalanadi
-Uzatuvchi va qabul qiluvchi bir necha kalitlardan foydalanadi
-Uzatuvchi ikkita kalit va qabul qiluvchi bitta kalitdan foydalanadi

?
321.Tomonlar simmetrik shifrlashda shifrlash algoritmini qanday tanlashadi?
+Xabar almashinuvini boshlash oldidan
-Xabar almashinuvi boshlagandan keyingi holat
-Xabar almashinish mobaynida
-Xabar almashishdan keyin

?
322.Simmetrik shifrlash algoritmida axborot almashinuvi nechta bosqichda amalga oshiriladi?
+3 bosqichda
-4 bosqichda
-5 bosqichda

-2 bosqichda

?
323.ATM texnologiyasining zaifligi nimada?
+Foydalanuvchi axborotini va ma'lumotlar marshrutini noqonuniy o'zgartirish
-Virtual aloqa subyektlarining birini g'arazli almashtirishning qonuniy kurinishi
-Axborot uzatishni cheklab qo'yish
-Axborot uzatish tezligining kamaytirilishi

?
324.IP Security - buÖ
+IP-paketlarni yetkazishda ularning himoyasini ta'minlash, autentifikatsiya va shifrlash masalalariga taalluqli protokollar toíplami
-OSI tarmoq modelining kanal pogíonasi protokoli
-Parolli himoya samaradorligi parollarning sir saqlanish darajasiga bog'liq
-Boshlang'ich ma'lumotlarga bir tomonlama o'zgartirish funksiyasini qo'llash yoíli bilan olingan baytlar toíplami

?
325.Transport rejimi ñ bu Ö
+Amaliy xizmatlar axborotini o'zida mujassam etgan transport pog'onasi (TCP, UDP, ICMP) protokollarini o'z ichiga oladigan IP paket ma'lumotlar maydonini shifrlash uchun qo'llaniladi
-Butun paketni, shuningdek, tarmoq pog'onasi sarlavhasini ham shifrlashni ko'zda tutadi kup protokollarini o'z ichiga oladigan IP paket ma'lumotlar maydonini shifrlash uchun qo'llaniladi
-Trafik xavfsizligini ta'minlash xizmatlari taqdim etadigan ulanish
-Boshqaruvning juda egiluvchan mexanizmidir va u har bir paketni qayta ishlashda juda qo'l keladi

?
326.Tunel rejimi ñ bu Ö
+Butun paketni, shuningdek, tarmoq pog'onasi sarlavhasini ham shifrlashni ko'zda tutadi
-Trafik xavfsizligini ta'minlash xizmatlari taqdim etadigan ulanish va deshifrlash jaroyonini urganish
-Boshqaruvning juda egiluvchan mexanizmidir
-IP paket ma'lumotlar maydonini shifrlash uchun qo'llaniladi

?
327.Xavfsizlik siyosati ma'lumotlar ombori ñ bu
+Boshqaruvning juda egiluvchan mexanizmidir va u har bir paketni qayta ishlashda juda qo'l keladi
-Amaliy xizmatlar axborotini o'zida mujassam etgan transport pog'onasi (TCP, UDP, ICMP) protokollarini o'z ichiga oladigan IP paket ma'lumotlar maydonini shifrlash uchun qo'llaniladi
-Butun paketni, shuningdek, tarmoq pog'onasi sarlavhasini ham shifrlashni ko'zda tutadi
-Trafik xavfsizligini ta'minlash xizmatlari taqdim etadigan ulanish

?
328.Birga qo'llaniladigan kalitli autentifikatsiya ñ bu Ö
+Mijoz punkti va kirish nuqtasi WEP ni qo'llab-quvvatlashi va bir xil WEP-kalitlarga ega bo'lishi kerak
-Ochiq matnli chaqiruv freymi bilan javob beruvchi kirish nuqtasi
-Autentifikatsiya algoritmining qo'llanilishini ko'rsatuvchi signal va bir xil WAN-kalitlarga ega bo'lishi kerak
-Erkin (nol) autentifikatsiyali algoritm

?
329.Himoya strategiyasi ñ bu Ö
+Mezonlarni, ayniqsa tezkor mezonlarni rasmiy aniqlash
-Hisoblash texnikasi vositasi
-Oldindan aniqlangan mezonlar bilan erkin kuzatish
-Amalga oshirishga bog'liq bo'lmagan xavfsizlik talablari

?
330.3G tarmoqlarida axborot xavfsizligini ta'milanlashning maqsad va prinsiplari nima?
+Jahon miqyosida xavfsizlikni ta'minlash usullarini yetarli darajada standartlashtirishni ta'minlash. Bu turli xizmat koírsatish tarmoqlari oírtasida rouming va oízaro aloqani amalga oshirishi kerak
-2G xavfsizlik tizimida aniqlangan kamchiliklarni hisobga olgan holda 3G tizimlar xavfsizligi chora tadbirlarini mukammallashtirish. Bu turli xizmat koírsatish tarmoqlari oírtasida rouming va oízaro aloqani amalga oshirishi kerak
-UMTS axborot xavfsizligini ta'minlash 2G tarmoqlari uchun ishlab chiqilgan mexanizmlarga asoslanadi

-Qo'shimcha xavfsizlik usullarodan foydalanish ehtimoli

?
331.UMTS xavfsizligini ta'minlashning ustunligi va prinsiplari qanday prinsiplarga asoslangan?
+3G tizimlarida 2G xavfsizligini ta'minlash elementlaridan foydalanish shartga
-3G xavfsizlik tizimida aniqlangan kamchiliklarni hisobga olgan holda 2G tizimlar xavfsizligini taíminlashning yangi usullarini ishlab chiqishga
-UMTS xavfsizlik tizimida aniqlangan kamchiliklarni hisobga olgan holda 3G tizimlar xavfsizligi chora tadbirlarini mukammallashtirishga
-3G tizimlar xavfsizligini ta'minlash va 2G tizimlardagi taklif etiladigan yangi xizmatlar xavfsizligini ta'minlashning yangi usullarini ishlab chiqishga

?
332.3G UMTS tizim xavfsizligini ta'minlash uchun 2G tizim xavfsizligining quyidagi qaysi jihatlarini bartaraf etish kerak?
+Yo'lg'on qabul qilgich-uzatgich baza stansiyasi BTSdan foydalanib amalga oshiriladigan faol tahdidlar ehtimoli
-Autentifikatsiya ma'lumotlari va shifr kalitlarni tarmoqlararo va tarmoq ichida yashirin uzatish
-Xalqaro mobil aloqa apparatining identifikatori IMEI xavfsizlik tahdidlaridan himoyalangan
-UMTS xavfsizlik tizimida aniqlangan kamchiliklarni hisobga olgan holda 3G tizimlar xavfsizligi chora tadbirlarini mukammallashtirish

?
333.Tarmoq sohasining xavfsizligi nima?
+Nazorat jurnalidagi ro'yxat bilan muvofiq bo'lgan qalloblikni aniqlash va xavfsizlik bilan bog'liq bo'lgan hodisalarga taalluqli axborotni tahlil etish uchun taqdim etish
-Ro'yxat paytida, abonentlar pul to'lamasdan xizmatlardan foydalangandagi frod (qalloblik)
-Mobil qurilmaning xalqaro identifikatsion raqami IMEI ni identifikatsiyalash va ma'lumotlar butunligi Bu turli xizmat koírsatish tarmoqlari oírtasida rouming va oízaro aloqani amalga oshirishi kerak
-Foydalanuvchi va tarmoq autentifikatsiyasi

?
334.3G mobil telekommunikatsiyalar tizimi xizmatlaridan foydalanuvchining xavfsiz foydalanishi. Bu guruhga kiradigan xavfsizlik metodlari nimalarni taíminlaydi?
+Foydalanuvchi identifikatorining konfidentsialligi, tarmoq va foydalanuvchi autentifikatsiyasini va ma'lumotlar konfidentsialligini
-Foydalanuvchi identifikatorining butunligini
-Ro'yxat paytida, abonentlar pul to'lamasdan xizmatlardan foydalangandagi frodni (qalloblik)
-Foydalanuvchilar ma'lumotlar trafigi konfidentsialligining buzilishi riskiga olib keladigan ushlashni

?
335.Konfidentsallikning buzulishi buÖ
+Buzgíunchi shaxsiy maílumotlar saqlanadigan maílumotlar ombori servisiga kirishga ruxsat olishi mumkun
-Markaziy stansiya unsurlari ustidan boshqarishni taminlash uchun Middleware- servisini ishlatishni taminlaydi
-Uzatilayotgan trafigda kiritilgan oízgartirishlar va ruxsatsiz kirishning bazi misollarini oíz ichiga oladi
-Bu xar qanday faoliyat,oxirgi foydalanuvchi xavsizlikning etarli darajasiz IPTV xizmatiga ega boladi

?
336.Autendifikatsiyaning asosiy vazifalariÖ
+Identefikatorlarni va ishlatiluvchi dekodr manzillarini haqiqiyligini tasdiqlovchi, xamda smartcard va dekodrlarni buyriqlar oqimi tasiridan himoya qilish
-Axborot provayder servislariga yakka xolda va guruxlashgan manzil operatsiyalarini ishlab chiqarish imkoniyatini beradi va dekodrlarni buyriqlar oqimi tasiridan himoya qilish
-Markaziy stansiya unsurlari ustidan boshqarishni taminlash uchun Middleware- servisini ishlatishni taminlaydi
-Oxirgi foydalanuvchi xavsizlikning etarli darajasiz IPTV xizmatiga ega boladi

?
337.Himoya qilish mexanizmini quyda keltirilgan hujjatlardan qaysi birida toíg'íri taírif berilgan?
+Test asosida hujjatlashtirish ñ tizim ishlab chiquvchi himoyalash vositalari tizimi administrator yoíriqnomasi, loyiha asosida hujjatlashtirish, hujjatlarni koírib chiqishi kerak
-Test asosida hujjatlashtirish ñ himoya qilish tamoyillarini tafsiflash va ularni tizimda joriy qilish
-Loyiha asosida hujjatlashtirish - tizim ishlab chiquvchi testlash rejasi va jarayonini tafsiflovchi hujjatlarni koírib chiqishi kerak va dekodrlarni buyriqlar oqimi tasiridan himoya qilish
-Himoya qili vositalarida tizim haxfsizlik yoíriqnomasi

?
338.Taxdidlarni tahlil qilish jarayoni qanday bosqichlardan iborat?
+Axborot resurslarni identifikatsiyalash, baholash mezonlarini tanlash va zaiflikni baholash
-Axborot resurslarini autentifikatsiyalash
-Baholash mezonlarini tanlash va ilova va resurslarga potentsial ijobiy ta'sir etishni aniqlash
-Zaiflik jihatlarini aniqlash va ilova va resurslarga potentsial ijobiy ta'sir etishni aniqlash

?
339.Kriptografik metodlar an'anaviy tarzda qanday konfidentsial axborotni shifrlash uchun qo'llaniladi?
+Aloqa tarmoqlari boíylab uzatiladigan yozma matnlar, xabarlar va dasturiy ta'minotni
-Yozma matnlar, grafika va raqamlarni
-Dasturiy ta'minot, grafika, ovoz yoki harflarni va yozma matnlar, xabarlar va dasturiy ta'minotni
-Dasturiy ta'minot, grafika yoki ovozni

?
340.Virtual kanal boshqaruv madeli nimalarga bogíliq?
+Amalga oshiriladigan kirish matritsasiga
-Obyekt va subyektning roíyxat qilingan maílumotlariga
-Obyekt va subyektning identifikatoridan
-Kirish dispetcheriga

?
341.Qanday usul lokal tarmoqqa masofadan kirishning samarali usulidir?
+Internet global tarmog'i orqali kirish
-Telefon tarmog'i orqali kirish
-Axborotni uzatish muhiti orqali kirish
-Telegraf tarmog'i orqali kirish

?
342.Qanday protokollarga masofadagi foydalanuvchilarning tarmoqqa kirishini markazlashgan boshqaruv protokollari deyiladi?
+TACACS, RADIUS
-TACACS, FTP (UDP, WEP)
-RADIUS,TCP
-ICMP, IP

?
343.TACACS qaysi pratokolga asoslangan?
+TCP
-IPX
-UDP
-ICMP

?
344.RADIUS qaysi pratokolga asoslangan?
+TCP
-IPX
-UDP
-ICMP

?
345.Radius autendifikatsiyaning qaysi turini qoíllab-quvvatlamaydi?
+ARAP
-ASCII
-PAP
-CHAP

?
346.Insoniylik omiliga taaluqli boílmagan tahdid turi nima?
+Parol tizimini ishdan chiqarish
-Esda qoladigan va yengil topiladigan parolni tanlash
-Qiyin parolni yozish va kerakli joyda saqlash
-Begonalar koíradigan qilib parolni kiritish

?
347.1986 yil nashr etilgan Sazerland ximoya modeli nimaga asoslangan?
+Axborot oqimiga va subíektlar oízaro taísir kuchiga
-Tizimning bir xolatdan boshqa xolatga oítishiga
-Obíektlarga subíyektlar kirish huquqini shakllantirish va tranzaktsiyalarfan foydalanishga
-Avtomatlar nazariyasi asosiga

?
348.Tarmoqlararo ekranlar qaysi oilaga mansub protokollarda ishlaydi?
+TCP/IP
-IPX/SPX
-OSI
-ISO

?
349.Axborotni oílchash birligi?
+Bit
-Bod
-Bit/s
-Erlahg

?
350.Wi-Fi uzatish tezligi?
+54 Ãbit/s gacha
-44 Mbit/s gacha
-34 Mbit/s gacha
-24 Ãbit/s gacha
?
351.Wi-MAX uzatish tezligi?
+75 Ãbit/s
-55 Ãbit/s
-65 Ãbit/s
-45 Ãbit/s

?
352.Uzatish boíyicha modemlar qnday turlarga boílinadi?
+Sinxron va asinxron
-Ichki va tashqi
-Guruxli va portativ
-Parallel va ketma-ket

?
353.MUTning sifat tavsiflari?
+Toígírilik va ishonchlilik
-Modulyatsiya tezligi

-Xavfsizlik
-Toígírilik, ishonchlilik va xavfzizlik

?
354.Butunlikni taíminlash uchun koíp qoíllaniladigan shovqinbardosh kodlarni keltiring?
+Xemming kodi, BCHX kodlari, Fayra kodi, Rid-Solomon kodlari
-Tsiklik kodlar
-Toígíirlovchi kodlar va Deffi Helman pratokollari (turli sinflar uchun)
-Ortiqcha kodlar

?
355.Axborot butunligini taíminlash usullaridan birini keltiring?
+Raqamli imzo va imitoqoíyilma
-Kodlash va dekodlash
-Impulsli-kodli axborot va uning funksiyasi
-Raqamli imzo

?
356.Xavfsizlik deganda ... {
-dushman tomonga uyushtiriladigan hujumga tushuniladi.
+shaxsning, korxonaning, davlatning muhim hayotiy manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati tushuniladi.
-shaxsning, korxonaning, davlatning noqonuniy foyda koërishdan ximoyalanganlik holati tushunilali tashqi tahdidlardan himoyalanganlik holati tushuniladi.
-uyushtirilmagangan hujumga qarshi hujum uyushtirish tushuniladi.
?
357.Axborotga murojaat qilish imkoniyatini taíminlash nimani anglatadi?{
+ Belgilangan vakt oraligida vaqolatga ega boëlgan axborot foydalanuvchilari va subíektlari uchun axborot yoki u bilan bogëliq servisga murojaat qilib foydalanish imkoniyatini taíminlashni anglatadi.
- Saqlanayotgan axborot vaqolatga ega boëlmagan subíektlar tomonidan oëzgartirilishidan, yaíni axborot tuzilishi va maínosi qanday berilgan boëlsa, shunday saqlashni taíminlashni va vazivalarini anglatadi.
- Axborotga vaqolati boëlmagan subíektlar tomonidan murojaat qilib, undan oshkor holda foydalanishdan ximoya qilishni anglatadi.
- Uzatilayotgan axborot oëzgartirilgan holda boëlsa ham joydagi foydalanuvchiga kelib tushishi imkoniyatini taíminlash tushuniladi.
?
358.Axborotning statik yaxlitligi deganda ...{
- axborotlarni kayta ishlash jarayonida bir axborotni kayta ishlash natijasida toëgëri natijaviy axborot olinib, oëzgartirilmagan holda tegishli boëginga etkazilishi tushuniladi
- komp¸yuter xotirasiga kiritilgan maílumotning kodlashtirilishi tushuniladi va axborotni kayta ishlash natijasida toëgëri natijaviy axborot olinib, oëzgartirilmagan holda tegishli boëginga etkazilishi tushuniladi
+ belgilangan obíekt xaqidagi maílumotlar oëzgarmay saqlanishi tushuniladi.
- axborotning komp¸yuter xotirasidan chikarish qurilmasiga kayta shifrlanib chikarilishi tushuniladi.
?
359.tahdid deganda ...{
+ kimlarningdir manfaatlariga ziyon etkazuvchi roëy berishi mumkin boëlgan voqea, taísir, jarayon tushuniladi.
- hujumni amalga oshirishga qaratilgan harakat tushuniladi.
- zaifliklarni aniklash va undan foydalanish choralarini ishlab chikish tushuniladi.
- Xali sodir etilmagan, lekin sodir etilishi kutilayotgan voqea yoki jarayon tushuniladi, taísir, jarayon tushuniladi.
?
360.Axborot munosabatlari subíektlari manfaatlariga qaratilgan tahdid deb nimaga aytiladi? {
- Axborot tizimi foydalanuvchilariga nisbatan ishlatiladigan zuravonlik va kuch ishlatishga aytiladi va taísir, jarayon tushuniladi.
+ Axborotga yoki axborot tizimiga salbiy taísir etuvchi potensial roëy berishi mumkin boëlgan voqea yoki jarayon aytiladi.
- Axborot tizimi infrastrukturasiga nisbatan amalga oshiriladigan quporuvchilik harakatlariga aytiladi.
- Barcha javoblar toëgëri.
?
361.Foydalanuvchilarning voz kschishlari natijasida kelib chikadigan tahdidlar ...{
- belgilangan tartib va qoidalarga rioya qilmaslikdan, ataylab yoki tasodifan harakatlar tufayli tizimning ishdan chikishidan, yul quyilgan xatoliklar va nosozliklardan kelib chikadi.
- dasturiy va texnik taíminotdagi uzilish va nosozliklardan kelib chikadi.
- tashqi xotirada saqlanayotgan maílumotlarninkslib chikadi.

+ axborot tizimi bilan ishlash xoxishining yukligi, kasbiy tayyorgarlik saviyasi pastligi, normal sharoitning yukligidan kelib chikadi.
?
362.Zarar etkazuvchi dasturlar qaysi jixatlari bilan ajralib turadilar? {
+ Buzish funksiyasi bilan, tarqalish usuli bilan, tashqi kurinishi bilan.
- Tabiiy ravishda joriy etilishi bilan, tizimni bir zumda ishdan chikarishi bilan.
- Juda tez tarqalishi bilan, murakkab buyruklardan iboratligi bilan.
- Inson salomatligiga taísiri bilan.
?
363.Axborot tizimlarida axborot xavfsizligini taíminlashga oid raxbariyat tomonidan kabul qilingan chora-tadbirlar qaysi bugëinga tegishli? {
- xuquqiy bugëinga
+ maímuriy bugëinga
- amaliy bugëinga
- dasturiy va texnik bugëinga
- Barcha bugëinlarga
?
364."Axborotlashtirish toëgërisida"gi Qonunning nechanchi moddasi "Axborot resurslari va axborot tizimlarini muxofaza qilish" nomi bilan atalgan?{
+ 19-moddasi
- 3-moddasi
- 10-moddasi
- 20-moddasi
?
365.Turli davlatlarning axborot xavfsizligi buyicha standartlash bazalarining shakllanishiga nima asos boëldi?{
- Evropa davlatlari - Fransii, Germanii, Niderlandiya va Buyuk Britaniya vakillarining hamkorlikda ishlab chikilgan ìUygunlashtirilgan mezonlarî asos boëldi.
- "Axborot texnologiyalarida axborot xavfsizligini baxolash mezonlari" nomli ISO/IEC 15408 standart asos boëldi.
+ Dunyoda birinchi boëlib AQSH da yaratilgan va keng koëlamda foydalanilgan "Ishonchli komp¸yuter tizimlarini baxolash mezonlari" nomli standarti asos boëldi.
- Axborot xavfsizligi masalalarini toëliq va chukur talkin kiluvchi, keyinchalik shartli ravishda X.800 nomi berilgan texnik xususiyatlar asos boëldi.
?
366."Oranjevaya kniga"da ishonchlilikning qaysi pogëonalari keltirilganî{
- 2 pogëonasi ó V va A belgilangan. V ishonchlilik darajasi past, A ishonchlilik darajasi yuqori boëlgan tizimlar uchun moëljallangan.
- 3 pogëonasi A, V, S pogëonalari belgilangan. A ishonchlilik darajasi past, S yuqori boëlgan gizimlar uchun moëljallangan.
- 5 pogëonasi ñ I, II, III va V belgilangan. I pogëona ishonchlilik darajasi yuqori, V pogëona past boëlgan tizimlar uchun moëljallangan B pogëonasi yuqori talablarga javob beruvchi tizimlar uchun moëljallangan.
+ 4 pogëonasi - D, S, V va A belgilangan. D pogëonasi ishonchlilik darajasi past va talabga javob bermaydigan tizimlar, A pogëonasi yuqori talablarga javob beruvchi tizimlar uchun moëljallangan.
?
367.Axborotlarni ximoyalashning almashtirish usullari moxiyati nimadan iborat? {
+ Tizimda saqlanayotgan axborot aloka liniyalari buyicha uzatilishida maílum koidaga kura kodlashtirilib, undan ochik holda bevosita foydalanish imkoniyati barataraf etiladi.
- Maxsus texnik ishlanmalar asosida axborotni kayta ishlovchi qurilmalar va vositalarda axborotni nazorat qilish va ximoya qilishni taíminlash ó amalga oshiriladi va uni vazifasini bajaradi
- Aloka kanallarini ximoya qilishda, keraksiz va xalakit kiluvchi elektromagnit nurlarini bartaraf etiladi.
- Axborot tizimidagi jarayonlarda va dasturlardan foydalanishda faoliyat kursatuvchi personalii nazorat qilish! amalga oshiriladi.
?
368.Biometrik vositalarda aniqlashning kvazistatik uslubi yordamida Ö{
+ foydalanuvchi kul geometriyasi yoki kuz xususiyatlari yoki qul izlari nusxasi yoki qon tomirlari rasmiga karab aniqlanadi.
- foydalanuvchi barmok izlarining nusxasi yoki yuz tuzilishi nazorat qilinib, aniqlanadi.
- foydalanuvchi pul¸si, ballistokardiografiya, ensefalografiya natijalari nazorat qilinib aniqlanadi.
- foydalanuvchi tovushi yoki yozuv shakli yoki bosmalash (pechatlash) stili nazorat qilinib aniqlanadi.
?
369.Elektron xujjat ayirboshlashni ximoyalashda uning yaxlitligini va begonalar tomonidan foylalanish imkoniyatidan saqlashii taíminlashda qaysi usul va vositalar kullaniladi?{
- Elektron rakamli imzo va Kriptografik usullar
- Biometrik usullar
- Bayonnomalar analizatorlar, Kriptografik usullari
+ hamma javoblar toëgëri.

?
370.Troyan dasturlari...{
- boshqa dasturlarga joriy etilib, zararlangan fayllarni ishga tushirishni boshqarish maqsadida ularga uzlarining kodlarini kiritadilar va maílumotlarni uchiradilar, tizimning ìosilibî qolishiga olib keladilar, maxfiy axborotlarni ugirlaydilar va xokazo.
+ komp¸yuterda foydalanuvchining ruxsatisiz maílum amallarni bajarishga kirishadilar, yaíni maílum sharontlarda diskdagi maílumotlarni uchiradilar, tizimning ìosilibî qolishiga olib keladilar, maxfiy axborotlarni ugirlaydilar va xokazo.
- tarmoq buyicha boshqa komp¸yuterlar adreslarini xisoblab, shu adreslar buyicha uz nusxalarini yuboradilar.
- komp¸yuterda foydalanuvchi ruxsati bilan maílum amallarni bajaradilar, yaíni ma¸lum fayllardan nusxa kuchiradilar, papka ichiga yangi fayl kiritadilar va xokazo.
?
371.Joriy etilish usuliga koëra viruslar ..{
- faylga, yuklovchi dasturlarga va bir vaktning oëzida ham fayl, ham yuklovchi dasturlarga joriy etiluvchi turlarga boëlinadilar.
+ rezident va norezident viruslarga ajratiladilar.
- chalgëitib, xalal beruvchi, xavfli boëlmagan va xavfli turlarga ajratiladilar.
- ìyuldoshî, fayl tizimi strukturasidagi, stele va ìruxî viruslarga ajratiladilar.
?
372.Virus signaturasi -ó ... {
+ virusning barcha nusxalarida va faqat nusxalarida uchraydigan kod boëlagi boëlib,maílum uzunlikka egadir.
- virusning oëzini-oëzi shifrlash xususiyatidir.
- virusning oëzini tizimda yashiruvchi boëlagi boëlib, bir papkadan ikkinchisiga sakrab oëtadi va va hokozo davom etadi
- virusning oshkor ravishda foydalanuvchi tomonidan aniqlanishi mumkin boëlgan boëlagidir.
?
373.Komp¸yuterning virus bilan zararlanishining nisbiy alomatlaridan qaysi biri notoëgëri? {
+ Tashqi xotira resurslariga umuman murojaat qilish imkoniyati yukligi.
- Komp¸yuterda avval kiska vakt ichida ishga tushuvchi biror dasturning juda sekinlik bilan ishga tushishi.
- Operatsion tizimning yuklanmasligi.
- Baízi kerakli fayl va papkalarning yuqolib qolishi yoki ular sigëimlarining oëzgarishi.
?
374.YOlgëon salbiy ogoxlantirishda...{
+antivirus dasturi xech kanday virus yukligi xaqida maílumot beradiku, lekin aslida tizimda virus xaqiqatan ham mavjud buladi.
-antivirus dasturi tizim normal holda ishlayotganligi xaqida maílumot beradi.
-antivirus dasturi tizimda jiddiy buzilishlar mavjudligi xaqida ogoxlantiruvchi maílumotlar beradi.
-antivirus dasturi foydalanuvchiga tizimda virus mavjudligi xaqida maílumot beradiku, lekin aslida bunday virus mavjud boëlmaydi.
?
375.SAM fayli qaerda saqlanadi? {
- Komp¸yuter administratorining seyfida.
+ Winnt_root\System32\Config tkatalogi ichida saqlanadi.
- Progra Files\Comon Files\ODBS katalogi ichida saqlanadi.
- CMOS xotirada saqlanadi.
?
376.MS Word 2002 da faylni ochish uchun parolli ximoya parametrlarini oërnatish ketma-kstligini aniqlang.
- Bosh menyudan Fayl > Soxranit¸ > fayl nomi va paroli kiritilib > OK bosiladi.
- Bosh menyuning Servis > Ustanovit¸ za˘itu > ´Zapretit¸ lyub˚e izmeneniya[a] bandi belgilanib, parol¸ kiritiladi va tasdiqlanadi.
+ Bosh menyudan Servis > Parametr˚ > ´Bezopasnost¸,[a], ´Parol¸ dlya otkr˚tiya fayla[a] maydoniga faylni ochish uchun parol¸ maílumotini kiritib, tasdiqlash kerak.
- Bosh menyudan Servis > Parametr˚ > ´Soxranenie[a], ´Parol¸ dlya otkr˚tiya fayla[a] maydoniga faylni ochish uchun parol¸ maílumotini kiritib, tasdiqlash kerak va tahlillash
?
377.MS Exsel XR da aktiv varaq (List) da yacheykalar ichidagi maílumotlarni va diagramma maílumotlarini ximoyalash uchun kanday ish tutish kerak?{
- Servis > Za˘ita > Za˘itit¸ list buyruklar kstma-ketligi bajarilib, ochilgan oynadan ximoya qilinadigan obíektlar belgilanadi va parol¸ maílumoti kiritiladi.
+ Servis > Za˘ita > Za˘itit¸ list buyruklar ketma-ketligi bajarilib, ochilgan oynadan ximoya qilinmaydigan obíektlar belgilanadi va parol¸ maílumoti kiritiladi.
- Servis > Bezopasnost¸ > Za˘ita > Za˘itit¸ list buyruklar ketma-ketligi bajarilib, ochilgan oynadan ´Obíekt˚[a] bandi belgilanib, parol¸ maílumoti kiritiladi.
- Fayl > Soxranit¸ > Servis > Parametr˚ > Za˘itit¸ list ketma-ketligini bajarib ochilgan oynada ´Soderjimoe[a] bandi belgilanib, parol¸ maílumoti kiritiladi.

?
378.Bradmauerlaning ulanish darajasida ishlovchi turlari ...{
+ishlash jarayonida kiruvchi va chikuvchi trafik maílumotlarini oëziga koëchirib oladilar va ular orkali tashqi tarmoqka ulanish mumkinmi yoki yukligini aniklaydilar.
-Internetning muayyan xizmat turi buyicha cheklashlarni amalga oshirishib xavfsizlikni taíminlaydilar va ular orkali tashqi tarmoqka ulanish mumkinmi yoki yukligini aniklaydilar.
-xavfsizlikni kelayotgan paketlarni fil¸trlash yuli bilan taíminlaylilar.
-Xavfsizlikni tarmoq komponentalari monitoringini uztkazib borish asosida taíminlaydilar.
?
379.Lokal tarmoqka Internet orkali uyushtiriladigan paketlar snifferi hujumi.. {
-xaker-buzgunchi tarmoq joylashgan korporatsiya xududida yoki uning tashqarisidan turib uzini tarmoqka kirish uchun vaqolati bor mutaxassis qilib kursatishi orkali amalga oshiriladi.
-tarmoq operatsion tizimi tashqil etuvchilarining ki tegishli dasturlarning 3 buzilishi natijasida tarmoq tizimiga vaqolatga ega boëlgan foydalanuvchilarning kirishi tusib kuyilishi maqsadida uyushtirladi.
+tarmoq kartasidan foydalanib fizik kanal orkali yuborilayotgan barcha axborot pakstlarini kayta ishlash maqsadida maxsus dasturga yuborish maqsadida uyushtiriladi.
-vaqolatga ega boëlgan foydalanuvchining tarmoqka kirishi uchun belgilangan parol maílumotini koëlga kiritish maqsadida uyushtiriladi.
?
380.Lokal tarmoqdagi trafikni oshkor qilish ... {
+tarmoq buyicha uzatilayotgan maílumotni ruxsatsiz egallab, undan foydalanish ski 8 boshqalarga oshkor qilishga urinishlarida roëy beradi.
-ruxsati boëlmagan foydalanuvchilar tomonidan tasodifan yoki gëarazli ravishda kerakli fayl va dasturlarga oëzgartirishlar kiritishga harakat qilishlari natijasida roëy beradi.
-boshqa foydalanuvchi tomonidan asl junatuvchi nomini qalbakilashtirib maílumot uzatish uchun amalga oshiriladigan harakatlar natijasida roëy beradi.
-tarmoqning muxim buginlarida resurslarga murojaat qilish imkoniyati yukligidan yoki apparat va dasturiy taíminot nosozligi tufayli roëy beradi.
?
381.Buzgunchilarning internet tarmogëi boëyicha hujum uyushtirishlari muvafffakiyatli amalga oshirilishining sabablaridan biri ... {
+kanal buyicha uzatilayotgan maílumotlarni osonlikcha kuzatish imkoni mavjudligi
-internet Exrlorer kabi brauzer dasturi interfeysining mukammal ishlanmaganligi
-operatsion tizim komponentalarining notoëgëri sozlanganligi
-Internetga ulanishlagi modem qurilmasi imkoniyatlari pastligi
?
382..... troyan dasturlari turkumiga mansub boëlib, komp¸yuterga masofadan viruslar orkali yoki boshqa yullar bilan joriy etiladilar. Nuktalar urniga mos javobni tanlang.{
-Viruslar
-CHuvalchanglar va boshqalar
-Fishing maílumotlari
+Botlar
?
383.Qaysi xizmatlar seanlari davomida uzatilayotgan maílumotlar osonlikcha buzgëunchilar tomonidan qulga kiritiladilar?{
+Elektron pochta, TELNET va FTR xizmatlarida
-UseNet va ETR xizmatlaridan va pochta xiznarlari
-TelNet va WWW xizmatlaridan
-WWW va UseNet xizmatlaridan
?
384.Axborot yigëish uchun yuborilgan spamda kanday maílumotlar beriladi? {
-Foydalanuvchining bankdagi xisob rakami oëzgarganligi xaqidagi maílumot yuborilib, uni aniqlashtirish maqsadida eski xisob rakamini tasdiqlash soëraladn.
-Majburiy toëlovlarni tulash xaqidagi maílumotlar yuboriladi.
+Soërov baxona biror bir anketa tuldirilishi talab etiladi va anketani kursatilgan manzilga yuborish soëraladi.
-U yoki bu tovarni xarid qilishga undovchi takliflar beriladi.
?
385.Web-serverlarda tarmoqni ximoya qilishdagi zaifliklar nima tufayli xosil buladi?{
-Web-serverlarda tarmoqni ximoya qilishdagi zaifliklar deyarli yuk, shuning uchun ular xavfsizlikni bartaraf eta oladilar.
+Serverga oërnatilgan ixtiyoriy skript xatoliklari tufayli maxalliy tarmoqni ximoya qilishdagi zaifliklar kelib chikadi.
-Web -serverdan foydalanuvchilarning malakalari past boëlganligi tufayli.
-Web -server oërnatilgan komp¸yuter tezkorligi talabga javob bera olmasligi tufayli.
?
386.Axborot xavfsizligi deb... {

-axborot tizimidagi ó axborotlarning turli shaxslarlan bekitilib ximoyalanganlikka aytiladi.
-axborot tizimi subíektlarining va tashkil etuvchilarining xolatini saqlashga aytiladi.
+axborot tizimida tasodifiy yoki gëarazli ravishda axborot egasiga yoki uning foydalanuvchisiga ziyon etkazuvchi xurujlardan ximoyalanganlikka aytiladi.
-axborotlarning boshqa subíektlarga berib yuborilishini oldini olish tushuniladi.
?
387.Axborotning dinamik yaxlitligi deganda ...{
-belgilangan obíekt xaqidagi maílumotlar oëzgarmay saqlanishi tushuniladi.
+axborotlarni kayta ishlash jarayonida bir axborotni kayta ishlash natijasida toëgëri natijaviy axborot olinib, oëzgartirilmagan holda tegishli bugëinga etkazilishi tushuniladi.
-komp¸yuter xotirasiga kiritilgan maílumotning kodlashtirilishi tushuniladi.
-axborotning komp¸yuter xotirasidan chikarish qurilmasiga kayta shifrlanib chikarilishi gupguniladi.
?
388.Xavfli darcha deb ...{
+Zaifliklar maílum boëlgan vaktdan to ularni bartaraf etilgunga kadar boëlgan vakg oraligëiga aytiladi.
-Axborot tizimiga uyushtiriladigan hujum davomiyligiga aytiladi.
-Axborot tizimi resurslarini ugëirlab ketish uchun moëljallangan darchaga aytiladi.
-Axborot tizimi ishlayotgan komp¸yuter monitori ekranidagi dushmanga koërinib turgan maílumotlar darchasiga aytiladi.
?
389.Axborot munosabatlarini koëllab-koëvvatlovchi infrastrukturaning rad etishi nagijasida kelib chikadigan tahdidlar ... {
- Belgilangan tartib va koidalarga rioya qilmaslikdan, ataylab yoki tasodifan harakatlar tufayli tizimning ishdan chikishidan, yul quyilgan xatoliklar va nosozliklardan kelib chikadi.
- Aloka, elektr taíminoti, suv va issiklik taíminoti, sovutish tizimlaridagi nosozliklardan kelib chikadi.
- Xonalar va ularlagi jixozlarning buzilishi, avariya xolatiga kelishi natijasida vujuldga keladi.
+ b va c javoblar toëgëri.
?
390."Davlat sirlarini saqlash borasidagi burch, ularni oshkor etganlik yoki konunga xilof ravishda maxfiylashtirganlik uchun javobgarlik" nomli modda qaysi xujjatda yoritilgan {
+Konstitutsiyada
-"Davlat sirlarini saqlash toëgërisida" gi qonunda
-"Axborot olish kafolatlari va erkinligi toëgërisida" gi qonunda
-Jinoyat qodeksida
?
391.Axborot xavfsizligida ´xavfsizlik siyosatiª - ... {
-axborotni oëgëirlanib, yuk qilinishi oldini olishga qaratilgan chora-tadbirlar guruxi.
-korxona yoki kompaniyada komp¸yuter foydalanuvchilariga tushuntiriladigan koërsatmalar.
+axborotni toëplash, kayta ishlash va tarkatishni tashqil etishga qaratilgan konunlar, koidalar va meíyoriy xujjatlar toëplami.
-axborot tizimi arxitekturasi va joriy etilishida unga boëlgan ishonchlilik mezoni buyicha beriladigan baxo.
?
392.Komp¸yuter virusiga xos boëlmagan xususiyatni aniqlang. {
-Maílum dasturlash tilida yaratilgan buyruklar ketma-ketligi.
-Bajariladigan fayllar, dasturlarga, tizimli soxaga joriy etilib, oëz nusxasini kupaytiradi va tarqaladi
+Komp¸yuter qurilmalari tomonidan faollashtirilib, ishga tushiriladi.
?
393.Buzish imkoniyatiga koëra viruslar ... {
+chalgëitib, xalal beruvchi, xavfli boëlmagan va xavfli turlarga ajratiladilar.
-rezident va norezident viruslarga ajratiladilar.
-faylga, yuklovchi dasturlarga va bir vaktning oëzida ham fayl, ham yuklovchi dasturlarga joriy etiluvchi turlarga boëlinadilar.
-kompan¸on, fayl tizimi strukturasidagi, stels va îruxî viruslarga ajratiladilar.
?
394.Operatsion tizim xavfsizligini taíminlash uchun kuyidagi tavsiyalardan qaysi biri toëgëri? {
-Bir paroldan bir necha foydalanuvchi oëz faoliyatila foydalanishdariga ruxsat berish mumkin.
+Komp¸yuterlar ishga tushiryalishida BIOS maílumotlariga oëzgartirishlar kiritishni taqiqlash maqsadida uning parolli ximoyasini oërnatish.
-Parol uzunligi iloji boricha ixcham boëlib, esga olish oson boëlgan belgilardan tuzilishi kerak.
-Parolda fakat xarfli belgilardan foylalanii kerak.
?
395.MS Word XR da ìServisî > ìParametr˚î >îBezopasnost¸î >"Ustanovit¸ za˘ituî õbuyruqlar ketma-ketligi yordamida kanday ximoyani oërnatish mumkin?{
-Xujjatni ochishning parolli ximoyasini oërnatib, undagi matnninig kurinishini shifrlab, oëzgartirish.
-Xujjat faylini tashqi xotiraga boshqa nom bilan saqlashni taqiqlashta qaratilgan ximoyani.
+Xujjatni taxrirlash yoki tekshirib unga tuzatish maílumotlari kistiriladigan xollarda boshqa oëzgartirishlar kiritilishini oldini

olish uchun parolli ximoyalashni
-Xujjat faylini bir necha kismga ajratishdan taíkiklashga qaratilgan ximoyani.
?
396.MS Excel da aktiv varaq (List) ximoyasini oërnatish uchun qaysi ketma-ketlikdan foydalaniladi. {
+Servis > Za˘ita > Za˘itit¸ list ketma-ketligi bajarilib, ochilgan oynadan ximoyalash parametrlari belgilanib, oërnatiladi.
-Servis > Bezopasnost¸ > Za˘ita > Za˘itit¸ list ketma-ketligini bajarib, ochilgan oynadan ximoyalash parametrlari belgilanib, oërnatiladi.
-Fayl > Soxranit¸ > Servis > Parametr˚ > Za˘itit¸ list buyruklar ketma-ketligi bajarilib, ximoyalash parametrlari belgilanib, oërnatiladi.
-Pravka> Za˘ita > List buyruklar ketma-ketligi bajariladi.
?
397.MS Exsel XR da makroviruslardan ximoyalanish uchun qaysi ketma-ketlikni bajarish kerak?{
-Servis > Bezopasnost¸ makrosov > Ustanovit¸ za˘itu mos ximoya darajasini belgilash kerak.
+Servis > Makros > Bezopasnost¸ ketma-ketligini bajarib, ochilgan oynada ´Uroven¸ bezopasnosti[a] ining ´V˚sokaya[a] darajasini tanlash kerak
-Fayl > Soxranit¸ kak > Servis > Ob˘ie parametr˚ > Za˘ita ot makrosov > ximoyaning mos darajasini belgilash kerak.
-Servis > Ustanovit¸ za˘itu > ´Zapretit¸ lyub˚e izmeneniya[a] bandi belgilanib parol¸ kiritiladi va tasdiqlanadi, Za˘ita ot makrosov > ximoyaning mos darajasini belgilash kerak.
?
398.Maílumotlaro bazasini shifrlash ... {
-ning samarasi juda past, sababi, buzgunchilar ularni osonlikcha buzib tiklashlari mumkin va boshqalar.
-fakat maxfiy axborotlarni ximoyalashdagina yuqori samara berishi mumkin.
-natijasida undagi ayrim obíektlar yashirin holda saqlanishi mumkin.
+natijasida maílumotlar bazasi boshqa dasturlar yordamida ochilishi va uqilishi taqiqlanadi.
?
399.Lokal tarmoqka Internet orkali uyushtiriladigan IP-spufing hujumi... {
+xiker-buzgëunchi tarmoq joylashgan korporatsiya xududida yoki uning tashkarisidan turib oëzini tarmoqka kirish uchun vaqolati bor mutaxassis qilib kursatishi orkali amalga oshiriladi.
-tarmoq kartasidan foydalanib fizik kanal orkali yuborilayotgan barcha axborot pakstlarini kayta ishlash maqsadida maxsus dasturga yuborish maqsadida uyushtiriladi.
-tarmoq operatsion tizimi tashkil etuvchilarining yoki tegishli dasturlarning buzilishi natijasida tarmoq tizimiga vaqolatga ega boëlgan foydalanuvchilarning kirishi toësib kuyilishi maqsadida uyushtirladi.
-vaqolatga ega boëlgan foydalanuvchining tarmoqka kirishi uchun belgilangan parol maílumotini kulga kiritish maqsadida uyushtiriladi.
?
400.Lokal tarmoqqa internet orkali uyushtiriladigan DoS hujumi ...{
-xaker-buzgëunchi tarmoq joylashgan korporatsiya xududida yoki uning tashkarisidan turib uzini tarmoqqa kirish uchun vaqolati bor mutaxassis qilib kursatishi orkali amalga oshiriladi va uning taxlillari urganiladi.
+tarmoq operatsion tizimi tashkil etuvchilarining yoki tegishli dasturlarnini buzilishi natijasida tarmoq tizimiga vaqolatga ega boëlgan foydalanuvchilarnin kirishi toësib kuyilishi maqsadida uyushtirladi.
-tarmoq kartasidan foydalanib fizik kanal orkali yuborilayotgan barcha axborot paketlarini kayta ishlash maqsadida maxsus dasturga yuborish maqsadila uyushtiriladi.
-vaqolatga ega boëlgan foydalanuvchining tarmoqqa kirishi uchun belgilangan parol maílumotini koëlga kiritish maqsadida uyushtiriladi.
401.Autentifikatsiya yordamida ...{
-tizimda ishlovchi sheriklar (foydalanuvchilar) xaqiqatan ham tizimda ishlash vaqolatiga ega ekanliklarini va maílumotlarning xakikiyligini tekshirish taíminlanadi.
-vaqolatga ega boëlmaganlar tarmoq axborot resurslariga murojaat qilishlariga ruxsat beriladi.
-komp¸yuter resurslari tekshirilib, taxlil qilinadi va bu paytda birorta foydalanuvchi unda ishlash imkoniga ega boëlmaydi.
+B va c javoblar toëgëri.
?
402.Axborot xavfsizligini taíminlashga qaratilgan ´Uygëunlashtirilgan mezonlar[a] ...{
-Dunyoda birinchi boëlib AQSH da yaratilgan va bunda keng koëlamda foydalanilgan "Ishonchli komp¸yuter tizimlarini baxolash mezonlari" nomli standart asos boëldi.
+Yevropa davlatlari - Fransii, Germanii, Niderlandiya va Buyuk Britaniya vakillarining hamkorligida ishlab chiqilgan boëlib, 1991 yilning iyun oyida eílon qilingan.
-"Axborot texnologiyalarida axborot xavfsizligini baxolash mezonlari" nomli ISO\IEC 15408 standarti asosida yaratilli.
-Axborot xavfsizligi masalalarini tulik va chukur talkin kiluvchi, keyinchalik unga shartli ravishda X.800 nomi berildi.
?
403."Axborot texnologiyalarida axborot xavfsizligini baxolash mezonlari" ISO\IEC 15408 standarti shartli ravishda qaysi nom bilan atalgan va unda ishonchlilik talablari nechta sinfdan iborat? {
-´Oranjevaya kniga[a], 55 ta sinfdan
-´Uygunlashtirilgan mezonlar[a], 20 ta sinfdan

-X.800, 10 ta sinfdan
+"Umumiy mszonlar", 10 ta sinfdan
?
404.Makroviruslar ...{
-operatsion tizimning baízi tashqil etuvchi komponentalarini - drayverlarni, uzilishlar roëy berishida faollashuvchi dasturlarni oëz kodlari bilan shunday almashtirib kuyadilarki, ular tizimda yakqol namoyon boëlmaydilar va kurinmaydilar.
+fakatgina fayllarni ochish yoki yopish jarayonida faol buladigan viruslar boëlib, ularning faolligi tizimda fayl bilan ishlayotgan dastur ishi tugagunicha davom etadi
-signaturasini turli xilda shifrlash xisobiga oëz kodini oëzgartirish xususiyatiga ega boëlgan viruslardir.
-jabrlanuvchi faylning bosh kismiga yoki oxiriga yozilib qolinadigan viruslardir.
?
405.YOlgon ijobiy ogoxlantirishda...{
+antivirus dasturi foydalanuvchiga tizimda virus mavjudligi xaqida maílumot beradiku, lekin aslida bunday virus mavjud boëlmaydi.
-antivirus dasturi xech kanday virus yoëkligi xaqida maílumot beradiku, lekin aslida tizimda virus xaqiqatan ham mavjud boëladi va boshqalar.
-antivirus dasturi tizim normal holda ishlayottanligi xaqida maílumot beradi.
-antivirus dasturi tizimda jiddiy buzilishlar mavjudligi xaqida ogoxlantiruvchi maílumotlar beradi.
?
406.Komp¸yuterning virus bilan zararlanishining bevosita alomatlaridan qaysi biri notoëgëri?{
+Operatsion tizim tarkibiga kiruvchi xizmatchi dasturning foydalanuvchiga virus bilan zararlanganlik xaqida maílumot etkazishi.
-Toësatdan komp¸yuter dinamiki orkali gëaroyib tovush signallarining eshitilishi.
-Komp¸yuterda qaysidir dastur yoki vazifa bilan ishlash jarayonida oëzidan-oëzi boshqa bir dasturning ishga tushib ketishi va tahlillanadi.
-Ekranga koëzda tutilmagan maílumotlar yoki tasvirlarning chikarilishi.
?
407.Farmer harakatlari davomiyligini aniqlang. {
-uzluksiz ravishda
-bir oylik vakt davomida
+1 yoki 2 kunlik qisqa vakt ichida
-bir xaftalik vakt oraligëida
?
408."Oranjevaya kniga"da ishonchlilikning qaysi pogëonalari keltirilganî{
-2 pogëonasi ó V va A belgilangan. V ishonchlilik darajasi past, A ishonchlilik darajasi yuqori boëlgan tizimlar uchun moëljallangan.
-3 pogëonasi A, V, S pogëonalari belgilangan. A ishonchlilik darajasi past, S yuqori boëlgan gizimlar uchun moëljallangan.
-5 pogëonasi ñ I, II, III va V belgilangan. I pogëona ishonchlilik darajasi yuqori, V pogëona past boëlgan tizimlar uchun moëljallangan.
+4 pogëonasi - D, S, V va A belgilangan. D pogëonasi ishonchlilik darajasi past va talabga javob bermaydigan tizimlar, A pogëonasi yuqori talablarga javob beruvchi tizimlar uchun moëljallangan.
?
409.Internet tarmogëidagi zaifliklardan biri - ...{
+aloka kanallari buyicha uzatilayotgan maílumotlarni osonlikcha kuzatish mumkinligi.
-maílumotlar uzatishning yagona protoqoli asosida butun jaxon mikyosidagi tarmoqlarning oëzaro bogëlanishi.
-lokal tarmoqdagi aloxida olingan ishchi stansiyadan bevosita Internet resurslariga murojaat qilish imkoniyati mavjudligi.
-kupgina foydalanuvchilar oëz faoliyatlarini Internetsiz tasavvur kila olmasliklari.
?
410.Spam bilan kurashishning dasturiy uslubida nimalar koëzda tutiladi?{
-Elektron pochta kutisiga kelib tushadigan spamlar meíyoriy xujjatlar asosida cheklanadi va bloklanadi
+Elektron pochta kutisiga kelib tushadigan ma¸lumotlar dasturlar asosida fil¸trlanib cheklanadi
-Elektron pochta kutisiga kelib tushadigan spamlar ommaviy ravishda cheklanadi
-Elektron pochta kutisiga kelib spamlar mintakaviy xududlarda cheklanadi.
?
411.Brandmauerlarning texnologik jixatlari buyicha kamchiliklaridan biri qaysi katorda keltirilgan? {
-Ular foylalanuvchining normal holda ishlashiga xalal beradilar.
-Internet tarmogëidan kelayotgan axborotlarning ayrimlarinigina nazorat qila oladilar.
-Foydalanuvchining elektron xatga biriktirilgan fayllardan ixtiyoriy tarzda foydalanish imkoniyatlarini yaratishlari
+Tizimning mehnat unumdorligiga taísiri
?
412.Windows XR brandmaueri nimalarga kodir emas?
-Bulayotgan jarayonlarni xisobga olib borishda (xavfsizlik jurnali yuritish).
+Spam maílumotlarini cheklash va ommaviy pochta xatlarini tarkatishning oldini olishga.

-Tashkaridan kelayottan viruslar va tarmoq chuvalchanglarini komp¸yuterlarga joriy etilishini toësishga.
-Hujumni tusish yoki bekor qilish uchun foydalanuvchidan tegishli koërsatmalar olishga.
?
413.Foydalanuvchilarning voz kechishlari natijasida kelib chikadigan tahdidlarÖ.{
-Belgilangan tartib va koidalarga rioya qilmaslikdan, ataylab yoki tasodifan harakatlar tufayli tizimni ishdan chiqishidan yoël qoëyilgan xatoliklar nosozliklardan kelib chikadi.
+Axborot tizimi bilan ishlash xoxishining yoëqligi, kasbiy tayyorgarliik saviyasi pastligi, normal sharoitning yuqligidan kelib chikadi.
-Dasturiy va texnik taíminotdagi uzilish va nosozliklardan kelib chikadi.
-Tashqi xotirada saqlanayotgan maílumotlarning buzilishidan kelib chikadi.
?
414.Komp¸yuter virusi -ó ... {
+boshqa dasturlarga suqilib kirib tarqalish imkoniyatiga ega boëlgan buyruklar ketma-ketligidan iborat kod.
-Hujum qilinayotgan tizim ustidan toëlik nazorat qilishni oëz zimmasiga ega boëlgan buyruklar ketma-ketligidan iborat kod.
-mustakil ravishda, yaíni boshqa dasturlarga suqilib kirmasdan oëz nusxalarini tizimda kupaytirish va bajarish imkoniyatiga ega boëlgan buyruklar ketma-ketligidan iborat kod.
-Inson salomatligiga xuruj kiluvchi unsurdir.
?
415.Qaysi xujjatda axborot borasidagi xavfsizlik tushunchasiga ´axborot soxasida shaxs jamiyat va davlat manfaatlarining ximoyalanganlik xolatiª, deb taírif berilgan? {
-´Axborotlashtirish toëgërisidaª Qonunda
-Oëzbekiston Respublikasi Konstitutsiyasida
+´Axborot erkinligi prinsiplari va kafolatlari toëgërisidaªgi Qonunda
-Rossiya Federatsiyasida kabul kilingan "Xalkaro axborot ayirboshlashda ishtirok etish toëgërisidaîgi qonunda
?
416.Oëzbekistonda zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish xuddi shuningdek maxsus virus dasturlarini ishlab chikish, ulardan qasddan foydalanish yoki ularni qasddan tarqatish xolati kayd qilinsa, kanday jazo choralari koëriladi?{
-Eng kam oylik ish xaqining etmish besh baravaridan ikki yuz baravarigacha mikdorda jarima yoki muayyan xukukdan maxrum qilib, uch oydan olti oygacha qamoq bilan jazolash.
+Eng kam oylik ish xakining yuz baravaridan uch yuz baravarigacha mikdorda jarima yoki ikki yilgacha ozodlikdan maxrum qilish bilan jazolanadi
-Eng kam oylik ish xakining etmish besh baravarigacha mikdorda jarima yoki uch yilgacha axloq tuzatish ishlari bilan jazolash.
-2 yildan 5 yilgacha ozodlikdan maxrum etish yoki zarar mikdorini qoplash bilan birga eng kam ish xakining 100 baravarigacha jarima.
?
417.Axborot xavfsizligi huquqiy bugëinidagi tadbirlarga qanday chora-tadbirlar kiradi?{
+Jamiyatda axborot xavfsizligi soxasi buyicha savodxonlikni va madaniyatni oshirishga qaratilgan chora-tadbirlar
-Axborot xavfsizligini taíminlashga qaratilgan vositalarni joriy etishga yunaltirilgan muvofiklashtiruvchi chora-tadbirlar.
-Xukukbuzarlik va axborot xavfsizligi buzgëunchilariga nisbatan jamiyatda salbiy munosabat shakllanishiga yunaltirilgan chora-tadbirlar
-Axborot borasidagi jinoyatlarni oldini olishga qaratilgan chora-tadbirlar ijodiy bidashuvni talab etadigan chora- tadbirlar
?
418.CHuvalchanglar ó...{
-boshqa dasturlarga suqilib kirib, tarqalish imkoniyatiga ega boëlgan buyruklar ketma-ketligidan iborat kod.
-hujum qilinayotgan tizim ustidan toëlik nazorat qilishni oëz zimmasiga oladigan buyruklar ketma-ketligidan iborat kod va va bajarish imkoniyatiga ega boëlgan buyruklar ketma-ketligdan iborat kod.
-biror predmet soxasiga tegishli axborotlar orasiga suqilib kiruvchi va oëz nusxasini kupaytiruvchi dastur kodi.
+mustakil ravishla, yaíni boshqa dasturlarga suqilib kirmasdan oëz nusxalarini tizimda kupaytirish va bajarish imkoniyatiga ega boëlgan buyruklar ketma-ketligdan iborat kod.
?
419.Axborot xavfsizligida kafolatlanganlik darajasi -{
+axborot tizimi arxitekturasi va joriy etilishida unga boëlgan ishonchlilik mezoni boëyicha beriladigan baho .
-axborotni toëplash, kayta ishlash va tarkatishni tashkil etishta qaratilgan konunlar, koidalar va meíyoriy xujjatlar toëplami.
-axborotni oëgëirlanib, yuk qilinishi oldini olishta qaratilgan ishonchli chora- tadbirlar guruxi.
-korxona yoki kompaniyada komp¸yuter foydalanuvchilariga tushuntiriladigan koërsatmalarning ular tomonidan ishonchli oëzlashtirilishi.
?
420.ìOranjevaya knigaîda berilgan axborot tizimlarining ishonchlilik darajasi boëyicha V pogëonasini kanday talqin etish mumkin? {
-Axborotga murojaat qilishii ixtiyoriy ravishda boshqarish.
+Axborotga murojaat qilishni majburan boshqarish.

-Oëzini-oëzi tekshiradigan va xavfsizlik taíminlanggan axborot tizimi.
-Xavfsizlikni taíminlashda tizimning barcha komponentalari va uning hayotiyssikli uchun konfiguratsion boshqarish.
?
421.Kuyidagilardan qaysi biri ´Taksimlangan tizimlarda axborot xavfsizligi. X.800ª
tavsiyalarida ksltirilmaganî?{
-Aulentifikatsiya qilish
-Axborotga murojaat qilishni boshqarish.
+Bajarilgan amallarni inkor etish.
-Axborot yaxlitligini taíminlash.
?
422.Ximoyalash vositalarini koëllashda tashkiliy tadbirlar nimalarni oëz ichita olishi kerak?{
-Tizimda saqlanayotgan axborotlar aloka liniyalari boëyicha uzatilishida maílum koidaga koëra kodlashtirilib, undan ochik holda bevosita foydalanish imkoniyati barataraf etish kabi tadbirlarni tartib-koidalariga katíiy rioya qilinishini taíminlash kabi tadbirlarni
+Axborot tizimidagi jarayoilarda va dasturlardan foydalanishda faoliyat koërsatuvchi personalni tanlash hamda nazorat qilish, axborotni kayta ishlash jaryonlarining tartib-koidalariga katíiy rioya qilinishini taíminlash kabi tadbirlarni
-Axborot tizimidagi jarayonlarda va dasturlardan foydalanishda barcha foydalanuvchilar uchun axborotga murojaat qilish imkoniyatini yaratishga qaratilgan tadbirlarni
-Axborot tizimidagi jarayonlarni va dasturlardan foydalanishni toëgëri tashqil etishii
?
423.Axborot tizimining tashkil etuvchilariga nisbatan boëladigan tahdidlarni aniqlang.{
+berilgan malumotlar, dasturlar, apparat qurilmalari va tizimni koëllab -koëvvatlovchi infrastrukturaga nisbatan boëladigan tahdidlar
-axborotga murojaat qilish imkoniyatiga karshi, axborotning yaxlitligini buzishga qaratilgan, axborotning maxfiyligini oshkor qilishga qaratilgan tahdidlar
-tabiiy, texnogen, tasodifiy, gëarazli maqsadda boëladigan taxdidlar
-ichki yoki tashqi taxdillar.
?
424.Axborotning maxfiyligini oshkor qilishga qaratilgan tahdidlarga ... {
-tizimga kirish uchun parol maílumotining buzgëunchi koëliga tushib qolishi kabi tahdid kiradi
-oëgërilik va qalloblik asosida boëladigan tahdidlar
-maílumotlarni egallab oliiiga qaratilgan tahdidlar kiradi.
-tabniy texnogen tahdidlar kiradi.
+hamma javob tug'ri.
?
425.Komp¸yuterning virus bilan zararlanishining nisbiy alomatlaridan qaysi biri notoëgëri?{
+Tashqi xotira resurslariga umuman murojaat qilish imkoniyati yukligi
-Komp¸yuterda avval qisqa vakt ichida ishga tushuvchi biror dasturning juda sekinlik bilan ishga tushishi.
-Operatsion tizimning yuklanmasligi.
-Baízi kerakli fayl va papkalarning yuqolib qolishi yoki ular sigëimlarini oëzgarishi.
-Komp¸yuter ishining tez-tez toëxtab, ìosilibî qolishi xolatlari.
?
426.Polimorf viruslar kanday viruslar?{
-Ular operatsion tizimning baízi tashkil etuvchi komponentalarini drayverlarini uzilishlar roëy berishida faollashuvchi dasturlarni oëz kodlari bilan shunday almashtirib kuyadilarki, ular tizimda yaqqol namoyon boëlmaydilar va koërinmaydilar
-Faqatgina fayllarni ochish yoki yopish jarayonida faol boëladigan viruslar boëlib ularning faolligi tizimda ishlayotgan dastur ishi tugagunicha davom etadi
+Signaturasini turli xilda shifrlash xisobiga oëz kodini oëzgartirish xususiyatiga ega boëlgan viruslar
-jabrlanuvchi faylning boshiga yoki oxiriga yozilib qoladigan viruslar
?
427.Viruslarni aniqlash usulidan qaysi biri keyingi paytlarla ishlatilmayapti{
+Immunizatorlar.
-Skanerlash usuli.
-Monitor usuli.
-Revizor usuli.
?
428.MS Word XR da ìServisî > ìParametr˚î >îBezopasnost¸î >"Ustanovit¸ za˘ituî õbuyruqlar ketma-ketligi yordamida kanday ximoyani oërnatish mumkin?{
+Xujjatni ochishning parolli ximoyasini oërnatib, undagi matnninig kurinishini shifrlab, oëzgartirish.
-Xujjat faylini tashqi xotiraga boshqa nom bilan saqlashni taqiqlashta qaratilgan ximoyani.
-Xujjatni taxrirlash yoki tekshirib unga tuzatish maílumotlari kistiriladigan xollarda boshqa oëzgartirishlar kiritilishini oldini olish uchun parolli ximoyalashni
-Xujjat faylini bir necha kismga ajratishdan taíkiklashga qaratilgan ximoyani.

?
429.MS Exsel XR da ìServisî > ìParametr˚î >îBezopasnost¸î` ketma-ketligi asosida kanday ximoyani oërnatish mumkin ?{
-Fakat ishchi kitobi faylini ochishiing parolli ximoyasini oërnatib, undagi jadvallar koërinishini shifrlab, oëzgartirishga qaratilgan ximoyani shifrlash algoritmini tanlash, makroviruslardan ximoyalanish parametrlarini oërnatish mumkin.
-Avval yaratilgan ishchi kitobi faylini tashqi xotiraga boshqa nom bilan saqlashni taqiqlashga qaratilgan ximoyani.
+Ishchi kitob faylini ochish, unga oëzgartirishlar kiritishning oldini olishning parolli ximoyasini, shifrlash algoritmini tanlash, makroviruslardan ximoyalanish parametrlarini oërnatish mumkin
-ishchi kitobi faylining aynan oëzini bir necha qismga ajratishdan taíqiqlashga qaratilgan himoyani.
?
430.MS Exsel da aktiv varaqni parol¸ yordamida ximoyalagach, varaq nomini oëzgartirish, varaqni umuman uchirish yoki uning oërnini boshqa joyga koëchirish mumkinmi? {
-Yuk, oëzgartirish mumkin emas, sababi u ximoyalangan.
+Xa, bemalol oëzgartirish mumkin.
-Varaq iomini oëzgartirish mumkin, lekin uni siljitish yoki oëchirish va oërnini almashtirish mumkin emas.
-Varaq nomini oëzgartirish mumkin, lekin uni siljitish yoki oëchirish mumkin.
?
431.Oëzbekistonda komp¸yuter axborotini modifikatsiyalashtirish fukarolarning xuquqlariga yoki qonun bilan quriqlanadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga koëp mikdorda zarar yoxud jiddiy ziyon stkazilishiga sabab boëlsa, kanday jazo choralari kuriladi?{
-Eng kam ish xakining 75 baravarigacha miqdorda jarima yoki 3 yilgacha ozodlikdan mahrum etish.
-3 yildan 6 yilgacha ozodlikdan mahrum etish.
+Eng kam oylik ish xakining yuz baravarigacha mikdorda jarima yoki bir yilgacha axlok tuzatish ishlari yoxud ikki yilgacha ozodlikdan mahrum qilish.
-2 yildan 5 yilgacha ozodlikdan maxrum etish yoki zarar mikdorini qoplash bilay birga eng kam ish xaqining 100 baravarigacha jarima.
?
432.Tarmoqka ruxsatsiz murojaat qilishshiig nechta modeli mavjud? {
-bitta modeli - boshqa foydalanuyachilar parollarini egallab olish
-ikki modeli - umumiy paroldan foydalanii, boshqa foydalanuvchilar parol maílumotlarini aniqlab olish tartib-koidalariga katíiy rioya qilinishini taíminlash kabi tadbirlarni
+uchta modeli - umumiy paroldan foydalanish, boshqa foydalanuvchilar parol maílumotlarini aniqlab olish va boshqa foydalanuvchilar parollarini egallab olish
-ikki modeli - umumiy paroldan foydalanish, boshqa foydalanuvchilar parollarini egallab olish
?
433.Identifikatsiya va asl foydalanuvchini aniklash xavfsizlik xizmati ó... {
+lokal tarmoqda fakat vaqolatga ega boëlgan foydalanuvchigina ishlashiga kafolat berishga yordam beradi.
-lokal tarmoq resurslariga belgilangan tartibdagi ruxsat buyicha murojaat qilinishida kafolat berilishiga yordam berali.
-lokal tarmoqdagi dasturlar va maílumotlar vaqolatga ega boëlmagan foydalanuvchilar tomonidan oshkor qilinmasligiga kafolat berishda yordam berali.
-tarmoq ishining buzilishidan ximoyalaydi.
?
434..... Internet tarmogëi orkali gëarazli maqsadlarda ma¸lumot yigëish, ularni buzgëunchilarga uzatish, yoki buzib yuborish kabi turli amallar bajarilishi hamda resurslarga masofadan turib murojaat qilish imkonini yaratadilar. Nuktalar urnini mos javob bilan toëldiring.{
-Virus dasturlari
+Troyan dasturlari
-CHuvalchanglar
-Fishing maílumotlari
?
435.Internet orkali masofada joylashgan komp¸yuterga yoki tarmoq resurslariga DoS- hujumlari uyushtirilishi natijasidaÖ..{
+foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan maxrum qilinadilar.
-foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzgëunchilarga etkaziladi.
-axborot tizimidagi maílumotlar bazalari oëgëirlanib koëlga kiritilgach, ular yuk qilinadilar.
-foydalanuvchilar axborotlariga ruxsatsiz oëzgartirishlar kiritilib, ularning yaxlitligi boëziladi.
?
436.Internet tarmogëida ishlashda foydalanuvchini oëziga oid maxfiy maílumotlarini boshqalarga oshkor qilishga majburan undash ... {
-bot deb ataladi.
-farming deb ataladi.
+fishing deb ataladi.
-reklama deb ataladi.
?
437.Internet tarmogëida ishlashda komp¸yuter mojarolarning aksariyat kupchiligi nima tufayli kelib chikkan? {

-Aloka kanallarda maílumot uzatilishi jarayonini kuzatib undagi parol¸ maílumotlari oëzlashtirish va uning monitoringlash
+Foydalanuvchi va tarmoq administratorlari tomonidan qabul qilingan statik parol¸ matlumotlarining soddaligi.
-Xost komp¸yuterlardagi Unix operatsion tizimi dasturlari oëzining ochik holdagi kodi bilan tarqatilganligi
-Barcha javoblar toëgëri.
?
438.Spamning oldini olish uchun kanday chora koërish tavsiya etiladi?{
+Elektron adres nomini saytning asosiy saxifasiga joylashtirmaslik. CHunki koëpgina spamerlar saytlarning dastlabki saxifalarini kurikdan utkazadilar.
-Elektron adres xaqidagi maílumotlarni Internetdagi forum yoki soërovlarda erkin bayon qilish.CHunki koëpgina spamerlar saytlarning dastlabki saxifalarini kurikdan utkazmaydilar.
-Internet orkali oldi-sotdi ishlarida elektron adresni kerakli tovar xarid sotib olishdagina maílum qilish.
-Elektron manzil nomini tez-tez oëzgartirib turish.
?
439.Bradmauerlaning paketli darajada ishlovchi turlari ...{
+xavfsizlikni kelayotgan paketlarni fil¸trlash yuli bilan taíminlaydilar.
-Internetning muayyan xizmat turi buyicha cheklashlarni amalga oshirishib xavfsizlikni taíminlaydilar.
-ishlash jarayonida kiruvchi va chikuvchi trafik maílumotlarini oëziga koëchirib oladilar va ular orkali tashqi tarmoqka ulanish mumkinmi yoki yukligini aniklaydilar.
-tarmoq komponsntalarini nazorati va monitoringini olib boradilar.
?
440.Bradmauerlarning paketli darajada ishlovchi turlarida Internet tarmogëi buyicha kelayotgan paketni maxalliy tarmoqka uzatish kerakligi yoki kerak emasligi nimalar asosida aniqlanadi?{
-URL-adres, oluvchining port nomeri va identifikatsion nomeri.
-Foydalanuvchi komp¸yuterining tarmoqdagi adresi, uning elektron pochta adresi, hamda filt¸rlash koidalari.
+IP-adres, junatuvchining port nomeri, bayroklar (belgilar).
-Internet xizmatiga oid protokol, joënatuvchi va oluvchi komp¸yuter adresi.
?
441.Foydalanuvchilarni turli omillar asosida autentifikatsiyalash, odatda foydalanuvchi biladigan va egalik qiladigan narsa asosida autentifikatsiyalash bu - .... .
+ikki faktorli autentifikatsiya
-autentifikatsiyaning klassik usuli
-kup martali parollash asosida autentifikatsiya
-biometrik autentifikatsiya
?
442.Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yoënaltirilgan buzgëunchi bu - ... .
{
+krakker
-xakker
-virus bot
-ishonchsiz dasturchi

№		Vopros 202 =79(1)+84(2)+39(3)
1		**Konfidensiallikni ta’minlash bu - ?**
	A)	Ruxsat etilmagan “o‘qishdan” himoyalash
	B)	Ruxsat etilmagan “yozishdan” himoyalash
	C)	Ruxsat etilmagan “bajarishdan” himoyalash
	D)	Ruxsat berilgan “amallarni” bajarish
2		**Foydalanuvchanlikni ta’minlash bu - ?**
	A)	Ruxsat etilmagan “bajarishdan” himoyalash
	B)	Ruxsat etilmagan “yozishdan” himoyalash
	C)	Ruxsat etilmagan “o‘qishdan” himoyalash
	D)	Ruxsat berilgan “amallarni” bajarish

3		**Butunlikni ta’minlash bu - ?**
	A)	Ruxsat etilmagan “yozishdan” himoyalash
	B)	Ruxsat etilmagan “o‘qishdan” himoyalash
	C)	Ruxsat etilmagan “bajarishdan” himoyalash
	D)	Ruxsat berilgan “amallarni” bajarish
4		**Hujumchi kabi fikrlash nima uchun kerak?**
	A)	Bo‘lishi mumkin bo‘lgan xavfni oldini olish uchun.
	B)	Kafolatlangan amallarni ta’minlash.
	C)	Ma’lumot, axborot va tizimdan foydalanish uchun.
	D)	Ma’lumotni aniq va ishonchli ekanligini bilish uchun.
5		**Tizimli fikrlash nima uchun kerak?**
	A)	Kafolatlangan amallarni ta’minlash.
	B)	Bo‘lishi mumkin bo‘lgan xavfni oldini olish uchun
	C)	Ma’lumot, axborot va tizimdan foydalanish uchun.
	D)	Ma’lumotni aniq va ishonchli ekanligini bilish uchun.
6		**Risk bu?**
	A)	Noaniqlikning maqsadlarga ta’siri
	B)	U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz
	C)	Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa
	D)	Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa
7		**Tahdid bu?**
	A)	Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa
	B)	Noaniqlikning maqsadlarga ta’siri
	C)	U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz
	D)	Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa
8		**Aktiv bu?**
	A)	Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa
	B)	Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa
	C)	Noaniqlikning maqsadlarga ta’siri
	D)	U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz
9		**Zaiflik bu?**
	A)	Bir yoki bir nechta tahdidga sabab bo‘luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik
	B)	Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa
	C)	Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa
	D)	Noaniqlikning maqsadlarga ta’siri
10		**Boshqarish vositasi bu?**
	A)	Riskni o‘zgartiradigan harakatlar bo‘lib, boshqarish natijasi zaiflik yoki tahdidga ta’sir qi
	B)	Bir yoki bir nechta tahdidga sabab bo‘luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik
	C)	Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa
	D)	Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa
11		**Har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilsa ....**
	A)	Risk paydo bo‘ladi.
	B)	Hujum paydo bo‘ladi.
	C)	Tahdid paydo bo‘ladi.
	D)	Aktiv paydo bo‘ladi.
12		**Denial of service (DOS) hujumi axborotni .... xususiyatini buzushga qaratilgan.**

	A)	Foydalanuvchanlik
	B)	Butunlik
	C)	Konfidensiallik
	D)	Ishonchlilik
13		**Tashkil etuvchilar xavfsizligi, aloqa xavfsizligi va dasturiy ta’minotlar xavfsizligi iborat bo‘lgan xavfsizlik sohasi bu?**
	A)	Tizim xavfsizligi
	B)	Ma’lumotlar xavfsizligi
	C)	Inson xavfsizligi
	D)	Tashkilot xavfsizligi
14		**Kriptologiya bu?**
	A)	“Maxfiy kodlar”ni yaratish va buzish fani va sanati
	B)	“Maxfiy kodlar”ni yaratish fani va sanati
	C)	“Maxfiy kodlar”ni buzish fani va sanati
	D)	Axborotni himoyalash fani va sanati
15		**.... kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi.**
	A)	Kalit
	B)	Ochiq matn
	C)	Alifbo
	D)	Algoritm
16		**Kriptografiya bu?**
	A)	“Maxfiy kodlar”ni yaratish fani va sanati
	B)	“Maxfiy kodlar”ni yaratish va buzish fani va sanati
	C)	“Maxfiy kodlar”ni buzish fani va sanati
	D)	Axborotni himoyalash fani va sanati
17		**Kriptotahlil bu?**
	A)	“Maxfiy kodlar”ni buzish fani va sanati
	B)	“Maxfiy kodlar”ni yaratish fani va sanati
	C)	“Maxfiy kodlar”ni yaratish va buzish fani va sanati
	D)	Axborotni himoyalash fani va sanati
18		**..... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to‘plami.**
	A)	Alifbo
	B)	Ochiq matn
	C)	Shifrmatn
	D)	Kodlash
19		**Agar ochiq ma’lumot shifrlansa, natijasi .... bo‘ladi.**
	A)	Shifrmatn
	B)	Ochiq matn
	C)	Nomalum
	D)	Kod
20		**Deshifrlash jarayonida kalit va ..... kerak bo‘ladi.**
	A)	Shifrmatn
	B)	Ochiq matn
	C)	Kodlash
	D)	Alifbo
21		**Ma’lumotni sakkizlik sanoq tizimidan o‘n oltilik sanoq tizimiga o‘tkazish bu?**
	A)	Kodlash
	B)	Shifrlash

	C)	Yashirish
	D)	Deshifrlash
22		**Ma’lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalanuvchi tizim bu?**
	A)	Simmetrik kriptotizim
	B)	Ochiq kalitli kriptotizim
	C)	Asimetrik kriptotizim
	D)	Xesh funksiyalar
23		**Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi?**
	A)	Ochiq kalitli kriptotizim
	B)	Simmetrik kriptotizim
	C)	Xesh funksiyalar
	D)	MAS tizimlari
24		**Ma’lumotni mavjudligini yashirishni maqsad qilgan bilim sohasi bu?**
	A)	Steganografiya
	B)	Kriptografiya
	C)	Kodlash
	D)	Kriptotahlil
25		**Ma’lumotni foydalanuvchiga qulay tarzda taqdim qilish uchun ..... zarur.**
	A)	Kodlash
	B)	Shifrlash
	C)	Yashirish
	D)	Deshifrlash
26		**Ma’lumotni konfidensialligini ta’minlash uchun ..... zarur.**
	A)	Shifrlash
	B)	Kodlash
	C)	Yashirish
	D)	Deshifrlash
27		**Ma’lumotni mavjudligini yashirish uchun .....**
	A)	Steganografiyadan foydalaniladi.
	B)	Kriptografiyadan foydalaniladi.
	C)	Kodlashdan foydalaniladi.
	D)	Kriptotahlildan foydalaniladi.
28		**Xesh funksiyalar bu?**
	A)	Kalitsiz kriptografik funksiya
	B)	Bir kalitli kriptografik funksiya
	C)	Ikki kalitli kriptografik funksiya
	D)	Ko‘p kalitli kriptografik funksiya
29		**Ma’lumotni uzatishda kriptografik himoya .....**
	A)	Konfidensiallik va butunlikni ta’minlaydi.
	B)	Konfidensiallik va foydalanuvchanlikni ta’minlaydi.
	C)	Foydalanuvchanlik va butunlikni ta’minlaydi.
	D)	Konfidensiallik ta’minlaydi.
30		**Qadimiy davr klassik shifriga quyidagilarning qaysi biri tegishli?**
	A)	Sezar shifri

	B)	Kodlar kitobi
	C)	Enigma shifri
	D)	DES, AES shifri
31		**Kompyuter davriga tegishli shifrlarni aniqlang.**
	A)	DES, AES shifri
	B)	Sezar shifri
	C)	Kodlar kitobi
	D)	Enigma shifri
32		**Chastotalar tahlili bo‘yicha quyidagilardan qaysi shifrlarni buzib bo‘lmaydi.**
	A)	O‘rin almashtirish shifrlarini.
	B)	Bir qiymatli o‘rniga qo‘yish shifrlarini.
	C)	Sezar shifrini.
	D)	Barcha javoblar to‘g‘ri.
33		**.... shifrlar blokli va oqimli turlarga ajratiladi.**
	A)	Simmetrik
	B)	Ochiq kalitli
	C)	Asimetrik
	D)	Klassik davr
34		**Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan shifrlash turi bu?**
	A)	Oqimli shifrlar
	B)	Blokli shifrlar
	C)	Ochiq kalitli shifrlar
	D)	Asimetrik shifrlar
35		**Ochiq matn qismlarini takror shifrlashga asoslangan usul bu?**
	A)	Blokli shifrlar
	B)	Oqimli shifrlash
	C)	Ochiq kalitli shifrlar
	D)	Asimetrik shifrlar
36		**A5/1 shifri qaysi turga mansub?**
	A)	Oqimli shifrlar
	B)	Blokli shifrlar
	C)	Ochiq kalitli shifrlar
	D)	Asimetrik shifrlar
37		**Qaysi algoritmlar simmetrik blokli shifrlarga tegishli?**
	A)	TEA, DES
	B)	A5/1, AES
	C)	Sezar, TEA
	D)	Vijiner, TEA
38		**Simmetrik kriptotizimlarning asosiy kamchiligi bu?**
	A)	Kalitni taqsimlash zaruriyati
	B)	Shifrlash jarayonining ko‘p vaqt olishi
	C)	Kalitlarni esda saqlash murakkabligi
	D)	Foydalanuvchilar tomonidan maqbul ko‘rilmasligi
39		**Faqat simmetrik blokli shifrlarga xos bo‘lgan atamani aniqlang?**
	A)	Blok uzunligi
	B)	Kalit uzunligi
	C)	Ochiq kalit
	D)	Kodlash jadvali

40		**Sezar shifrlash usuli qaysi akslantirishga asoslangan?**
	A)	O‘rniga qo‘yishga
	B)	O‘rin almashtirishga
	C)	Ochiq kalitli shifrlashga
	D)	Kombinatsion akslantirishga
41		**Qaysi akslantirishda ochiq matn va shifrmatndagi belgilarning chastotalari o‘zgarmaydi.**
	A)	O‘rniga qo‘yishga
	B)	O‘rin almashtirishga
	C)	Bunday akslantirish mavjud emas
	D)	Kombinatsion akslantirishga
42		**Kerxgofs prinsipiga ko‘ra kriptotizimning to‘liq xavfsiz bo‘lishi faqat qaysi kattalik nomalum bo‘lishiga asoslanishi kerak ?**
	A)	Kalit
	B)	Algoritm
	C)	Shifrmatn
	D)	protokol
43		**Shaxsiy kriptotizimlar nima uchun xavfsiz emas deb qaraladi.**
	A)	Tor doiradagi insonlar tomonidan ishlab chiqilgani va tahlil qilingani sababli
	B)	Faqat bitta kalitdan foydalanilgani sababli
	C)	Bardoshli kalitlardan foydalanilmagani sababli
	D)	Ikkita kalitdan foydalanilgani sababli
44		**Shifrlash va deshifrlash alohida kalitlardan foydalanuvchi kriptotizimlar bu?**
	A)	Ochiq kalitli kriptotizimlar
	B)	Simmetrik kriptotizimlar
	C)	Bir kalitli kriptotizimlar
	D)	Xesh funksiyalar
45		**Agar simmetrik kalitning uzunligi 128 bit bo‘lsa, jami bo‘lishi mumkin bo‘lgan kali soni nechta?**
	A)	2^{128}
	B)	128!
	C)	128^2
	D)	2^{127}
46		**Quyidagi shifrlar orasidan ochiq kalitli turga mansublarini tanlang.**
	A)	RSA
	B)	TEA
	C)	A5/1
	D)	Sezar
47		**Simmetrik shifrlar axborotni qaysi xususiyatlarini ta’minlashda foydalaniladi.**
	A)	Konfidensiallik va butunlik
	B)	Konfidensiallik
	C)	Butunlik va foydalanuvchanlik
	D)	Foydalanuvchanlik va konfidensiallik
48		**Ochiq kalitli shifrlar axborotni qaysi xususiyatlarini ta’minlashda foydalaniladi.**
	A)	Konfidensiallik va butunlik
	B)	Konfidensiallik
	C)	Butunlik va foydalanuvchanlik
	D)	Foydalanuvchanlik va konfidensiallik

49		**Rad etishni oldini oluvchi kriptotizimni aniqlang.**
	A)	Elektron raqamli imzo tizimi
	B)	MAS tizimlari
	C)	Simmetrik shifrlash tizimlari
	D)	Xesh funksiyalar
50		**Katt sonni faktorlash muammosiga asoslangan ochiq kalitli algoritmni aniqlang.**
	A)	RSA algoritmi
	B)	El-Gamal algoritmi
	C)	DES
	D)	TEA
51		**Ochiq kalitli kriptotizimlarning asosiy kamchiligini ko‘rsating?**
	A)	Hisoblashda yuqori vaqt sarflanadi
	B)	Kalitlarni taqsimlash muammosi mavjud
	C)	Ikkita kalitni saqlash muammosi mavjud
	D)	Foydalanish uchun noqulaylik tug‘diradi
52		**Ochiq kalitli kriptotizimlarni rad etishdan himoyalashining asosiy sababi nimada?**
	A)	Ikkita kalitdan foydalanilgani
	B)	Matematik muammoga asoslanilgani
	C)	Ochiq kalitni saqlash zaruriyati mavjud emasligi
	D)	Shaxsiy kalitni saqlash zarurligi
53		**MAS (Xabarlarni autentifikatsiya kodlari) tizimlari nima uchun rad etishdan himoya olmaydi?**
	A)	Yagona kalitdan foydalanilgani sababli
	B)	Xesh funksiyadan foydalanilgani sababli
	C)	Shaxsiy kalitni sir saqlanishi sababli
	D)	Faqat ma’lumot butunligini ta’minlagani sababli
54		**Xesh funksiyaga tegishli bo‘lmagan talabni aniqlang.**
	A)	Bir tomonlama funksiya bo‘lmasligi
	B)	Amalga oshirishdagi yuqori tezkorlik
	C)	Turli kirishlar turli chiqishlarni akslantirishi
	D)	Kolliziyaga bardoshli bo‘lishi
55		**Elektron raqamli imzoni shakllantirishda qaysi kalitdan foydalaniladi?**
	A)	Shaxsiy kalitdan
	B)	Ochiq kalitdan
	C)	Kalitdan foydalanilmaydi
	D)	Umumiy kalitdan
56		**Ochiq kalitli shifrlashda deshifrlash qaysi kalit asosida amalga oshiriladi?**
	A)	Shaxsiy kalit
	B)	Ochiq kalit
	C)	Kalitdan foydalanilmaydi
	D)	Umumiy kalit
57		**Elektron raqamli imzo quyida keltirilganlarning qaysi birini ta’minlaydi?**
	A)	Axborot butunligini va rad etishdan himoyalashni
	B)	Axborot konfidensialligini va rad etishdan himoyalashni
	C)	Axborot konfidensialligini
	D)	Axborot butunligini
58		**Ochiq kalitli kriptotizim asosida dastlab shifrlab so‘nga imzo qo‘yish sxemasida qay muammo mavjud?**

	A)	Shifrmatnni ixtiyoriy kishi imzolab yuborishi mumkin
	B)	Imzoni ixtiyoriy kishi tekshirishi mumkin
	C)	Osonlik bilan shifrmatnni kalitsiz deshifrlashi mumkinligi
	D)	Muammo mavjud emas
59		**Ochiq kalitli kriptotizim asosida dastlab imzo qo‘yib so‘nga shifrlash sxemasida qayday muammo mavjud?**
	A)	Deshifrlanganidan so‘ng imzolangan ma’lumotni ixtiyoriy kishiga yuborish mumkin.
	B)	Shifrmatnni ixtiyoriy kishi imzolab yuborishi mumkin
	C)	Imzoni ixtiyoriy kishi tekshirishi mumkin
	D)	Muammo mavjud emas
60		**Faqat ma’lumotni butunligini ta’minlovchi kriptotizimlarni aniqlang.**
	A)	MAS (Xabarlarni autentifikatsiya kodlari) tizimlari
	B)	Elektron raqamli imzo tizimlari
	C)	Ochiq kalitli shifrlash tizimlari
	D)	Barcha javoblar to‘g‘ri
61		**Quyida keltirilgan qaysi ketma-ketlik to‘g‘ri manoga ega.**
	A)	Identifikatsiya, autentifikatsiya, avtorizatsiya
	B)	Autentifikatsiya, avtorizatsiya, identifikatsiya
	C)	Identifikatsiya, avtorizatsiya, autentifikatsiya
	D)	Avtorizatsiya, identifikatsiya, autentifikatsiya
62		**Foydalanuvchini tizimga tanitish jarayoni bu?**
	A)	Identifikatsiya
	B)	Autentifikatsiya
	C)	Avtorizatsiya
	D)	Ro‘yxatga olish
63		**Foydalanuvchini haqiqiyligini tekshirish jarayoni bu?**
	A)	Autentifikatsiya
	B)	Identifikatsiya
	C)	Avtorizatsiya
	D)	Ro‘yxatga olish
64		**Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu?**
	A)	Avtorizatsiya
	B)	Autentifikatsiya
	C)	Identifikatsiya
	D)	Ro‘yxatga olish
65		**Biror narsani bilishga asoslangan autentifikatsiya usulining asosiy kamchiligi?**
	A)	Esda saqlash zaruriyati
	B)	Birga olib yurish zaririyati
	C)	Almashtirib bo‘lmaslik
	D)	Qalbakilashtirish mumkinligi
66		**Biror narsani bilishga asoslangan autentifikatsiyaga tegishli bo‘lgan misollarni aniqlang.**
	A)	PIN, Parol
	B)	Token, mashinaning kaliti
	C)	Yuz tasviri, barmoq izi
	D)	Biometrik parametrlar
67		**Biror narsaga egalik qilishga asoslangan autentifikatsiya usulining asosiy kamchilig**
	A)	Doimo xavfsiz saqlab olib yurish zaruriyati

	B)	Doimo esada saqlash zaruriyati
	C)	Qalbakilashtirish muammosi mavjudligi
	D)	Almashtirib bo‘lmaslik
68		**Esda saqlash va olib yurish zaruriyatini talab etmaydigan autentifikatsiya usuli bu?**
	A)	Biometrik parametrlarga asoslangan usuli
	B)	Parolga asoslangan usul
	C)	Tokenga asoslangan usul
	D)	Ko‘p faktorli autentifikatsiya usuli
69		**Eng yuqori darajagi universallik darajasiga ega biometrik parametrni ko‘rsating.**
	A)	Yuz tasviri
	B)	Ko‘z qorachig‘i
	C)	Barmoq izi
	D)	Qo‘l shakli
70		**Eng yuqori darajagi takrorlanmaslik darajasiga ega biometrik parametrni ko‘rsati**
	A)	Ko‘z qorachig‘i
	B)	Yuz tasviri
	C)	Barmoq izi
	D)	Qo‘l shakli
71		**Agar har ikkala tomonning haqiqiyligini tekshirish jarayoni bu?**
	A)	Ikki tomonlama autentifikatsiya
	B)	Ikki faktorli autentifikatsiya
	C)	Ko‘p faktorli autentifikatsiya
	D)	Biometrik autentifikatsiya
72		**Ko‘p faktorli autentifikatsiya bu?**
	A)	S va D javoblar to‘g‘ri
	B)	Har ikkala tomonni haqiqiyligini tekshirish darayoni
	C)	Birdan ortiq faktorlardan foydalanish asosida haqiqiylikni tekshirish
	D)	Barmoq izi va parol asosida haqiqiylikni tekshirish
73		**Biror narsani bilishga asoslangan autentifikatsiya usuliga qaratilgan hujuml ko‘rsating?**
	A)	Parollar lug‘atidan foydalanish asosida hujum, elka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum
	B)	Fizik o‘g‘irlash hujumi, elka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum
	C)	Parollar lug‘atidan foydalanish asosida hujum, elka orqali qarash hujumi, qalbakilashti hujumi
	D)	Parollar lug‘atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararli dasturlardan foydanish asosida hujum
74		**Biror narsaga egalik qilishga asoslangan autentifikatsiya usuliga qaratilgan hujuml ko‘rsating?**
	A)	Fizik o‘g‘irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujum
	B)	Parollar lug‘atidan foydalanish asosida hujum, elka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum
	C)	Fizik o‘g‘irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujum
	D)	Parollar lug‘atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararli dasturlardan foydanish asosida hujum
75		**Biometrik parametrga asoslangan autentifikatsiya usuliga qaratilgan hujuml ko‘rsating?**

	A)	Qalbakilashtirish, ba’lumotlar bazasidagi parametrlarni almashtirish
	B)	Fizik o‘g‘irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujum
	C)	Fizik o‘g‘irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujum
	D)	Qalbakilashtirish, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar
76		**Parollar bazada qanday ko‘rinishda saqlanadi?**
	A)	Xeshlangan ko‘rinishda
	B)	Shifrlangan ko‘rinishda
	C)	Ochiq holatda
	D)	Bazada saqlanmaydi
77		**Agar parolning uzunligi 8 ta belgi va har bir o‘rinda 256 ta turlicha belgidan foydalanish mumkin bo‘lsa, bo‘lishi mumkin jami parollar sonini toping.**
	A)	256^8
	B)	8^{256}
	C)	256!
	D)	2^{256}
78		**Parolni “salt” (tuz) kattaligidan foydalanib xeshlashdan (h(password, salt)) asosiy maqsad nima?**
	A)	Buzg‘unchiga ortiqcha hisoblashni talab etuvchi murakkablikni yaratish
	B)	Buzg‘unchi topa olmasligi uchun yangi nomalum kiritish
	C)	Xesh qiymatni tasodifiylik darajasini oshirish
	D)	Xesh qiymatni qaytmaslik talabini oshirish
79		**Qanday paroldan foydalanish tavsiya etiladi?**
	A)	Iboralar asosida hosil qilingan parollardan
	B)	Turli belgidan iborat va murakkab parollardan
	C)	Faqat belgi va raqamdan iborat parollardan
	D)	Faqat raqamdan iborat parollardan
80		**Fizik himoyani buzilishiga olib keluvchi tahdidlar yuzaga kelish shakliga ko‘ra qan guruhlarga bo‘linadi?**
	A)	Tabiy va sun’iy
	B)	Ichki va tashqi
	C)	Aktiv va passiv
	D)	Bir tomonlama va ko‘p tomonlama
81		**Quyidagilarnnig qaysi biri tabiy tahdidlar hisoblanadi?**
	A)	Yong‘in, suv toshishi, harorat ortishi
	B)	Yong‘in, o‘g‘irlik, qisqa tutashuvlar
	C)	Suv toshishi, namlikni ortib ketishi, bosqinchilik
	D)	Bosqinchilik, terrorizm, o‘g‘irlik
82		**Quyidagilarnnig qaysi biri sun’iy tahdidlar hisoblanadi?**
	A)	Bosqinchilik, terrorizm, o‘g‘irlik
	B)	Yong‘in, suv toshishi, harorat ortishi
	C)	Yong‘in, o‘g‘irlik, qisqa tutashuvlar
	D)	Suv toshishi, namlikni ortib ketishi, bosqinchilik
83		**Yong‘inga qarshi kurashishning passiv usuliga kiruvchi choralarni ko‘rsating**
	A)	Yong‘inga chidamli materiallardan foydalanish, zaxira xona va etajlarni qoldirish, tushuntiruv ishlarini olib borish
	B)	Yong‘inni aniqlash, agnishitel va qum yordamida o‘chirish
	C)	Yong‘inga chidamli materiallardan foydalanish, agnishitel va qum yordamida o‘chirish

	D)	Zaxira xona va etajlarni qoldirish, tushuntiruv ishlarini olib borish, yong‘in bo‘lganligi haqida signal berish
84		**Axborotni fizik xavfsizligini ta’minlashda inson faktorini mujassamlashtir nazoratlash usuli bu?**
	A)	Ma’muriy nazoratlash
	B)	Fizik nazoratlash
	C)	Texnik nazoratlash
	D)	Apparat nazoratlash
85		**Qaysi fizik to‘siq insonlarni tashkilotda faqat bittadan kirishini ta’minlaydi?**
	A)	Turniket
	B)	To‘mba
	C)	Metal zaborlar
	D)	Elektr zaborlar
86		**Faqat ob’ektning egasi tomonidan foydalanish imtiyozini nazoratlaydigan mant foydalanish usuli bu?**
	A)	Diskresion foydalanishni boshqarish
	B)	Mandatli foydalanishni boshqarish
	C)	Rolga asoslangan foydalanishni boshqarish
	D)	Attributga asoslangan foydalanishni boshqarish
87		**Ob’ektlar va sub’ektlarni klassifikatsiyalashga asoslangan foydalanishni boshqa usuli bu?**
	A)	Mandatli foydalanishni boshqarish
	B)	Diskresion foydalanishni boshqarish
	C)	Rolga asoslangan foydalanishni boshqarish
	D)	Attributga asoslangan foydalanishni boshqarish
88		**1. Agar sub’ektning xavfsizlik darajasida ob’ektning xavfsizlik darajasi mavjud bo‘ u holda o‘qish uchun ruxsat beriladi.** **2. Agar sub’ektning xavfsizlik darajasi ob’ektning xavfsizlik darajasida bo‘lsa, u ho yozishga ruxsat beriladi. Ushbu qoidalar axborotni qaysi xususiyatini ta’minlas qaratilgan?**
	A)	Konfidensiallikni
	B)	Foydalanuvchanlikni
	C)	Butunlikni
	D)	Ishonchlilikni
89		**1. Aagar sub’ektning xavfsizlik darajasida ob’ektning xavfsizlik darajasi mavjud bo‘ u holda yozish uchun ruxsat beriladi.** **2. Agar sub’ektning xavfsizlik darajasi ob’ektning xavfsizlik darajasida bo‘lsa, u ho o‘qishga ruxsat beriladi. Ushbu qoidalar axborotni qaysi xususiyatini ta’minlas qaratilgan?**
	A)	Butunlikni
	B)	Konfidensiallikni
	C)	Foydalanuvchanlikni
	D)	Maxfiylikni
90		**Foydalanishni boshqarishni tashkilotlardagi kadrlar toifasiga maksimal daraj yaqinlashtirishga harakat qilgan usul bu?**
	A)	Rolga asoslangan foydalanishni boshqarish
	B)	Mandatli foydalanishni boshqarish
	C)	Diskresion foydalanishni boshqarish

	D)	Attributga asoslangan foydalanishni boshqarish
91		**Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami bu?**
	A)	Rol
	B)	Imtiyoz
	C)	Daraja
	D)	Imkoniyat
92		**Qoida (rules), siyosat (policy), qoida va siyosatni mujassamlashtirgan algoritmlar (r combing algorithms), majburiyatlar (obligations) va maslahatlar (advices) k tushunchalar qaysi foydalanishni boshqarish usuliga aloqador.**
	A)	Attributga asoslangan foydalanishni boshqarish
	B)	Rolga asoslangan foydalanishni boshqarish
	C)	Mandatli foydalanishni boshqarish
	D)	Diskresion foydalanishni boshqarish
93		**Ushbu keltirilgan shart qaysi foydalanishni boshqarish usuliga tegishli: sub’ekt.Lavozimi=Vrach & muhit.vaqt >= 8:00 & muhit.vaqt <=18:00**
	A)	Attributga asoslangan foydalanishni boshqarish
	B)	Rolga asoslangan foydalanishni boshqarish
	C)	Mandatli foydalanishni boshqarish
	D)	Diskresion foydalanishni boshqarish
94		**Sug‘urta ma’lumotiga tegishli bo‘lgan …. quyidagi** $(\boldsymbol{Bob}, -), (\boldsymbol{Alisa}, \boldsymbol{rw}), (\boldsymbol{Sem}, \boldsymbol{rw}), (\boldsymbol{buxgalteriyaga\ oid\ dastur}, \boldsymbol{rw})$**. Nuqt o‘rniga mos atamani qo‘ying.**
	A)	Foydalanishni boshqarish ro‘yxati yoki ACL
	B)	Imtiyozlar ro‘yxati yoki C-list
	C)	Foydalanishni boshqari matritsasi
	D)	Biba modeli
95		**Alisaga tegishli ... quyidagiga te** $(\boldsymbol{OT}, \boldsymbol{rx}), (, \boldsymbol{buxgalteriyaga\ oid\ dastur}, \boldsymbol{rx}), (\boldsymbol{buxgalteriyaga\ oid\ ma'lumot},$ **Nuqtalar o‘rniga mos atamani qo‘ying.**
	A)	Imtiyozlar ro‘yxati yoki C-list
	B)	Foydalanishni boshqarish ro‘yxati yoki ACL
	C)	Foydalanishni boshqari matritsasi
	D)	Biba modeli
96		**Foydalanishni boshqarish matritsani ustunlar bo‘yicha bo‘lish va har bir ustunni m ob’ekt bilan saqlash orqali .... hosil qilinadi. Nuqtalar o‘rniga mos atamani qo‘ying.**
	A)	Foydalanishni boshqarish ro‘yxati yoki ACL
	B)	Imtiyozlar ro‘yxati yoki C-list
	C)	Foydalanishni boshqari matritsasi
	D)	Biba modeli
97		**Foydalanishni boshqarish matritsasini satrlar bo‘yicha saqlash va har bir satr mos sub’ekt bilan saqlash orqali .... hosil qilinadi. Nuqtalar o‘rniga mos atamani qo‘ying**
	A)	Imtiyozlar ro‘yxati yoki C-list
	B)	Foydalanishni boshqarish ro‘yxati yoki ACL
	C)	Foydalanishni boshqari matritsasi
	D)	Biba modeli
98		**Bell-Lapadula modeli axborotni qaysi xususiyatini ta’minlashni maqsad qiladi?**
	A)	Konfidensiallik
	B)	Butunlik

	C)	Foydalanuvchanlik
	D)	Ishonchlilik
99		**Biba modeli axborotni qaysi xususiyatini ta’minlashni maqsad qiladi?**
	A)	Butunlik
	B)	Konfidensiallik
	C)	Foydalanuvchanlik
	D)	Maxfiylik
100		**Biba modeliga ko‘ra agar birinchi ob’ektning ishonchlilik darajasi I(O1) ga teng bo va ikkinchi ob’ektning ishonchlilik darajasi I(O2) ga teng bo‘lsa, u holda ushbu ik ob’ektdan iborat bo‘lgan uchinchi ob’ektning ishonchlilik darajasi nimaga teng bo‘la Bu yerda, I(O1)>I(O2).**
	A)	I(O2)
	B)	I(O1)
	C)	I(O2) va I(O2) ga bog‘liq emas
	D)	Berilgan shartlash yetarli emas
101		**Bell-Lapadula modeliga modeliga ko‘ra agar birinchi ob’ektning xavfsizlik darajasi L(O1) ga teng bo‘lsa va ikkinchi ob’ektning xavfsizlik darajasi L(O2) ga teng bo‘lsa holda ushbu ikkita ob’ektdan iborat bo‘lgan uchinchi ob’ektning xavfsizlik darajasi nimaga teng bo‘ladi? Bu yerda, L(O1)>L(O2).**
	A)	L(O1)
	B)	L(O2)
	C)	L(O1) va L(O2) ga bog‘liq emas
	D)	Berilgan shartlar yetarli emas
102		**Agar biz O_1 ob’ektning butunligiga ishonsak, biroq O_2 ob’ektning butunlig ishonmasak, u holda ob’ekt O ikkita O_1 va O_2 ob’ektlardan yaratilgan bo‘lsa, u ho ob’ekt O ning butunligiga ishonmaymiz. Bu qaysi modelni anglatadi?**
	A)	Biba modelini
	B)	Bell-Lapadula modelini
	C)	Biror bir modelga tegishli emas
	D)	Biba va Bell-Lapadula modellari kombinatsiyasini.
103		**“Protsessorda shifrlash kalitini generatsiya qilish uchun maxsus kalit generatori mav bo‘lib, foydalanuvchi kiritgan parol asosida qulfdan yechiladi”. Gap qaysi turd shifrlash vositasi haqidi ketmoqda.**
	A)	Apparat
	B)	Dasturiy
	C)	Simmetrik
	D)	Ochiq kalitli
104		**“Shifrlashda boshqa dasturlar kabi kompyuter resursidan foydalanadi”. Gap qaysi turdagi shifrlash vositasi haqidi ketmoqda.**
	A)	Dasturiy
	B)	Apparat
	C)	Simmetrik
	D)	Ochiq kalitli
105		**Dasturiy ko‘rinishdagi shifrlash vositasi uchun mos bo‘lgan xususiyatni belgilang.**
	A)	Yangilash imkoniyati mavjud.
	B)	Shifrlash uchun saqlagishdagi (qurilmada) joylashgan maxsus protsessordan foydalanadi
	C)	Autentifikatsiya apparat qurilmaga nisbatan amalga oshiriladi
	D)	Qo‘shimcha drayver yoki dasturlarni o‘rnatishning hojati yo‘q

106		**Apparat ko‘rinishdagi shifrlash vositasi uchun mos bo‘lmagan xususiyatni belgilang**
	A)	Yangilash imkoniyati mavjud.
	B)	Shifrlash uchun saqlagishdagi (qurilmada) joylashgan maxsus protsessordan foydalanadi
	C)	Autentifikatsiya apparat qurilmaga nisbatan amalga oshiriladi
	D)	Qo‘shimcha drayver yoki dasturlarni o‘rnatishning hojati yo‘q
107		**Apparat ko‘rinishdagi shifrlash vositasi uchun mos bo‘lgan xususiyatni belgilang.**
	A)	Qo‘shimcha drayver yoki dasturlarni o‘rnatishning hojati yo‘q
	B)	Yangilash imkoniyati mavjud.
	C)	Parolni to‘liq tanlash hujumi yoki parolni topishga qaratilgan boshqa hujumlarga bardosh
	D)	Foydalanuvchi tomonidan kiritilgan parol ma’lumotni shifrlash kaliti sifatida foydalanila
108		**Diskni shifrlash usuliga xos bo‘lgan xususiyatlarni belgilang.**
	A)	Deyarli barcha narsa, almashtirish maydoni (swap space), vaqtinchalik fayllar, shifrlanad
	B)	Kalitlarni boshqarish, ya’ni, har bir fayl uchun turli kalitlardan foydalanish mumkin.
	C)	Faqat kriptografik kalitlar xotirada saqlanib, shifrlangan fayllar ochiq holatda saqlanadi.
	D)	asosiy fayl tizimining ustida joylashgan kriptografik fayl tizimidan foydalanish (masa ZFS, EncFS).
109		**Faylni shifrlash usuliga xos bo‘lgan xususiyatlarni belgilang.**
	A)	Kalitlarni boshqarish, ya’ni, har bir fayl uchun turli kalitlardan foydalanish mumkin.
	B)	Foydalanuvchi shaxsiy xabarlarni alohida shifrlashni unutgan vaqtlarda juda qo‘l keladi.
	C)	Zudlik bilan ma’lumotlarni yo‘q qilish uchun o‘rinli.
	D)	Deyarli barcha narsa, almashtirish maydoni (swap space), vaqtinchalik fayllar, shifrlanad
110		**Ma’lumotni xavfsiz yo‘q qilish nima uchun zarur?**
	A)	Ma’lumotni to‘liq konfidensialligini ta’minlash uchun
	B)	Ma’lumotni butunligini ta’minlash uchun
	C)	Ma’lumotni foydalanuvchanligini ta’minlash uchun
	D)	Xotirani bo‘shatish uchun.
111		**Qog‘oz ko‘rinishdagi ma’lumotni yo‘q qilish usullari orasidan quriq iqlimli sha uchun mos bo‘lmaganini aniqlang.**
	A)	Ko‘mish
	B)	Yoqish
	C)	Kimyoviy usul
	D)	maydalash (shreder)
112		**Ekologiyaga salbiy tasir qiluvchi, ortiqcha xarajatlarni talab etuvchi qog ko‘rinishdagi ma’lumotlarni yo‘q qilish usulini aniqlang.**
	A)	Yoqish
	B)	Ko‘mish
	C)	Kimyoviy usul
	D)	maydalash (shreder)
113		**Recuva, Wise Data Recovery, PC Inspector File Recovery, EaseUS Data Recovery Wizard Free, TestDisk and PhotoRec. Ushbu nomlarga xos bo‘lgan umumiy xususiyatni toping.**
	A)	Ularning barchasi ma’lumotni tiklovchi dasturiy vositalar.
	B)	Ularning barchasi bepul foydalaniluvchi dasturiy vositalar.
	C)	Ularning barchasi ma’lumotni xavfsiz o‘chiruvchi dasturiy vositalar.
	D)	Ularning barcha ma’lumotlarni zaxira saqlovchi dasturiy vositalar.
114		**Kriptografik kalit uzunligining o‘lchov birligi?**
	A)	Bit
	B)	Belgilar soni, ya’ni, ta

	C)	Kbayt
	D)	Metr
115		**Parol uzunligining o‘lchov birligi?**
	A)	Belgilar soni, ya’ni, ta
	B)	Bit
	C)	Kbayt
	D)	Metr
116		**Yaratish uchun biror matematik muammoni talab etadigan shifrlash algoritmi?**
	A)	Ochiq kalitli shifrlar
	B)	Simmetrik shifrlar
	C)	Blokli shifrlar
	D)	Oqimli shifrlar
117		**Xesh funksiyalarda kolliziya hodisasi bu - ?**
	A)	Ikki turli matnlarning xesh qiymatlarini bir xil bo‘lishi
	B)	Cheksiz uzunlikdagi axborotni xeshlay olishi
	C)	Tezkorlikda xeshlash imkoniyati
	D)	Turli matnlar uchun turli xesh qiymatlarni hosil bo‘lishi
118		**Xeshlangan ma’lumot nima deb ataladi?**
	A)	Xesh qiymat
	B)	Kalit
	C)	Shifrmatn
	D)	Parol
119		**Parol kalitdan nimasi bilan farq qiladi?**
	A)	Tasodifiylik darajasi bilan
	B)	Uzunligi bilan
	C)	Belgilari bilan
	D)	Samaradorligi bilan
120		**26 ta belgidan iborat Sezar shifrlash usilida kalitni bilmasdan turib nechta urinishd ochiq matnni aniqlash mumkin?**
	A)	25
	B)	26!
	C)	13
	D)	25^2
121		**Elektron raqamli imzoni muolajalarini ko‘rsating?**
	A)	Imzoni shakllantirish va imkoni tekshirish
	B)	Shifrlash va deshifrlash
	C)	Imzoni xeshlash va xesh matnni deshifrlash
	D)	Imzoni shakllartirish va xeshlash
122		**“Elka orqali qarash” hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.**
	A)	Biror narsani bilishga asoslangan autentifikatsiya.
	B)	Biror narsaga egalik qilishga asoslangan autentifikatsiya.
	C)	Biometrik autentifikatsiya.
	D)	Tokenga asoslangan autentifikatsiya
123		**Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usu qaratilgan.**
	A)	Biror narsani bilishga asoslangan autentifikatsiya.
	B)	Biror narsaga egalik qilishga asoslangan autentifikatsiya.
	C)	Biometrik autentifikatsiya.

	D)	Tokenga asoslangan autentifikatsiya
124		**Yo‘qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon**
	A)	Biror narsani bilishga asoslangan autentifikatsiya.
	B)	Biror narsaga egalik qilishga asoslangan autentifikatsiya.
	C)	Biometrik autentifikatsiya.
	D)	Tokenga asoslangan autentifikatsiya
125		**Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.**
	A)	Biometrik autentifikatsiya.
	B)	Biror narsani bilishga asoslangan autentifikatsiya.
	C)	Biror narsaga egalik qilishga asoslangan autentifikatsiya.
	D)	Tokenga asoslangan autentifikatsiya
126		**Elektron axborot saqlovchilardan qayta foydalanishli ma’lumotlarni yo‘q qi usullarini aniqlang.**
	A)	Qayta yozish va formatlash
	B)	Fizik yo‘q qilish
	C)	Maydalash (shredirlash)
	D)	Yanchish
127		**Elektron axborot saqlovchilardan ma’lumotni yo‘q qilishning qaysi usuli to kafolatlangan.**
	A)	Fizik yo‘q qilish
	B)	Qayta yozish
	C)	Formatlash
	D)	O‘chirish
128		**Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?**
	A)	Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan
	B)	Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhumligi bilan
	C)	Axborotni noqonuniy foydalanishlardan, o‘zgartirishlardan va yo‘q qilishlardan himoyalanganligi bilan
	D)	Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bil
129		**Axborotdan qanday foydalanish ruxsat etilgan deb yuritiladi?**
	A)	Foydalanishga o‘rnatilgan chegaralash qoidalarini buzmaydigan
	B)	Foydalanishga o‘rnatilgan chegaralash qoidalarini buzadigan
	C)	Axborot butunligini buzmaydigan
	D)	Axborot konfidensialligini buzmaydigan
130		**Axborotni butunligini ta’minlash usullarini ko‘rsating.**
	A)	Xesh funksiyalar, MAC
	B)	Shifrlash usullari.
	C)	Assimetrik shifrlash usullari, CRC tizimlari.
	D)	Shifrlash usullari, CRC tizimlari.
131		**Biba modeliga ko‘ra agar birinchi ob’ektning ishonchlilik darajasi I(O1) ga teng bo va ikkinchi ob’ektning ishonchlilik darajasi I(O2) ga teng bo‘lsa, u holda ushbu ik ob’ektdan iborat bo‘lgan uchinchi ob’ektning ishonchlilik darajasi nimaga teng bo‘la Bu yerda, I(O1)<I(O2).**
	A)	I(O1)
	B)	I(O2)
	C)	I(O2) va I(O2) ga bog‘liq emas
	D)	Berilgan shartlash yetarli emas
132		**Biba modeliga ko‘ra agar birinchi ob’ektning ishonchlilik darajasi I(O1) ga, ikki**

		ob’ektning ishonchlilik darajasi I(O2) ga va uchinchi ob’ektning ishonchlilik dara I(O3) teng bo‘lsa, u holda ushbu uchta ob’ektdan iborat bo‘lgan to‘rtinchi ob’ektn ishonchlilik darajasi nimaga teng bo‘ladi? Bu yerda, I(O1)>I(O2)> I(O3) .
	A)	I(O3)
	B)	I(O2)
	C)	I(O1)
	D)	Berilgan shartlash yetarli emas
133		**Bell-Lapadula modeliga modeliga ko‘ra agar birinchi ob’ektning xavfsizlik dara L(O1) ga teng bo‘lsa va ikkinchi ob’ektning xavfsizlik darajasi L(O2) ga teng bo‘ls holda ushbu ikkita ob’ektdan iborat bo‘lgan uchinchi ob’ektning xavfsizlik dara nimaga teng bo‘ladi? Bu yerda, L(O1)<L(O2).**
	A)	L(O2)
	B)	L(O1)
	C)	L(O1) va L(O2) ga bog‘liq emas
	D)	Berilgan shartlar yetarli emas
134		**Bell-Lapadula modeliga modeliga ko‘ra agar birinchi ob’ektning xavfsizlik dara L(O1) ga, ikkinchi ob’ektning xavfsizlik darajasi L(O2) ga va uchinchi ob’ektn xavfsizlik darajasi L(O3) teng bo‘lsa, u holda ushbu uchta ob’ektdan iborat bo‘l to‘rtinchi ob’ektning xavfsizlik darajasi nimaga teng bo‘ladi? Bu yer L(O1)<L(O2)<L(O3).**
	A)	L(O3)
	B)	L(O1)
	C)	L(O2)
	D)	Berilgan shartlar yetarli emas
135		**Elektron axborot saqlovchilardan qayta foydalanishli ma’lumotlarni yo‘q qilish usullari orasidan eng ishonchlisini aniqlang.**
	A)	Takroriy qayta yozish
	B)	Formatlash
	C)	Shift+Delete buyrug‘i yordamida o‘chirish
	D)	Delete buyrug‘i yordamida o‘chirish
136		**Quyida keltirilganlarning orasidan kompyuter topologiyalari hisoblanmaganla aniqlang.**
	A)	LAN, GAN, OSI
	B)	Yulduz, WAN, TCP/IP
	C)	Daraxt, IP, OSI
	D)	Shina, UDP, FTP
137		**OSI tarmoq modeli nechta sathdan iborat?**
	A)	7
	B)	4
	C)	6
	D)	5
138		**TCP/IP tarmoq modeli nechta sathdan iborat?**
	A)	4
	B)	7
	C)	6
	D)	5
139		**Quyidagilar orasidan qaysilari tarmoq turlari emas?**
	A)	Yulduz, WAN, TCP/IP

	B)	LAN, GAN
	C)	WAN, MAN
	D)	PAN, CAN
140		**Hajmi bo‘yicha eng kichik hisoblangan tarmoq turini ko‘rsating?**
	A)	PAN
	B)	LAN
	C)	CAN
	D)	MAN
141		**Qaysi topologiyada tarmoqdagi bir ishchi uzelning ishdan chiqishi butun tarmo ishdan chiqishiga sababchi bo‘ladi.**
	A)	Halqa topologiyada
	B)	Yulduz topologiyada
	C)	Shina topologiyada
	D)	Mesh topologiyada
142		**IPv4 protokolida IP manzil uchun necha bit ajratiladi.**
	A)	32
	B)	64
	C)	128
	D)	4
143		**IPv6 protokolida IP manzil uchun necha bit ajratiladi.**
	A)	128
	B)	32
	C)	64
	D)	4
144		**Domen nomlarini IP manzilga yoki aksincha almashtirishni amalga oshiruvchi xiz bu?**
	A)	DNS
	B)	TCP/IP
	C)	OSI
	D)	UDP
145		**Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi ularni uzib qo‘yuvchi oshkor bo‘lmagan hodisalarning potensial paydo bo‘lishi bu?**
	A)	Tahdid
	B)	Zaiflik
	C)	Hujum
	D)	Aktiv
146		**“Portlaganida” tizim xavfsizligini buzuvchi kutilmagan va oshkor bo‘lma hodisalarga olib keluvchi kamchilik, loyihalashdagi yoki amalga oshirishdagi xat bu?**
	A)	Zaiflik
	B)	Tahdid
	C)	Hujum
	D)	Kamchilik
147		**Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat bu?**
	A)	Hujum
	B)	Zaiflik
	C)	Tahdid
	D)	Zararli harakat

148		**Tarmoq xavfsizligi muammolariga olib kelmaydigan sababni aniqlang.**
	A)	Routerlardan foydalanmaslik
	B)	Qurilma yoki dasturiy vositani noto‘g‘ri sozlanishi
	C)	Tarmoqni xavfsiz bo‘lmagan tarzda va zaif loyihalash
	D)	Tug‘ma texnologiya zaifligi
149		**Tashkilot ichidan turib, xafa bo‘lgan xodimlar, g‘araz niyatli xodimlar tomoni amalga oshirilishi mumkin bo‘lgan tahdidlar bu?**
	A)	Ichki tahdidlar
	B)	Tashqi tahdidlar
	C)	Maxsus tahdidlar
	D)	Qastdan qilingan tahdidlar
150		**Tarmoq xavfsizligini buzulishi biznes faoliyatga qanday ta’sir qiladi?**
	A)	Biznes faoliyatning buzilishi, huquqiy javobgarlik
	B)	Axborotni o‘g‘irlanishi, tarmoq qurilmalarini fizik buzilishiga olib keladi
	C)	Maxfiylikni yo‘qolishi, tarmoq qurilmalarini fizik buzilishiga olib keladi
	D)	Huquqiy javobgarlik, tarmoq qurilmalarini fizik buzilishiga olib keladi
151		**Razvedka hujumlari bu?**
	A)	Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axbor to‘plashni maqsad qiladi.
	B)	Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.
	C)	Foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi.
	D)	Tizimni fizik buzishni maqsad qiladi.
152		**Kirish hujumlari bu?**
	A)	Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.
	B)	Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axbor to‘plashni maqsad qiladi.
	C)	Foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi.
	D)	Tarmoq haqida axborotni to‘plash hujumchilarga mavjud bo‘lgan potensial zaiflikni aniqlashga harakat qiladi.
153		**Xizmatdan vos kechishga qaratilgan hujumlar bu?**
	A)	Foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi.
	B)	Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.
	C)	Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axbor to‘plashni maqsad qiladi.
	D)	Tarmoq haqida axborotni to‘plash hujumchilarga mavjud bo‘lgan potensial zaiflikni aniqlashga harakat qiladi.
154		**Paketlarni snifferlash, portlarni skanerlash va Ping buyrug‘ini yuborish hujum qaysi hujumlar toifasiga kiradi?**
	A)	Razvedka hujumlari
	B)	Kirish hujumlari
	C)	DOS hujumlari
	D)	Zararli dasturlar yordamida amalga oshiriladigan hujumlar.
155		**“Bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsa yashiringan zararli koddan iborat bo‘ladi”. Bu xususiyat qaysi zararli dastur turiga**
	A)	Troyan otlari.
	B)	Adware
	C)	Spyware
	D)	Backdoors

156		**“Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘ rejimini kuzutib boradi”. Bu xususiyat qaysi zararli dastur turiga xos.**
	A)	Adware
	B)	Troyan otlari.
	C)	Spyware
	D)	Backdoors
157		**“Hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga ki imkonini beradi”. Bu xususiyat qaysi zararli dastur turiga xos.**
	A)	Backdoors
	B)	Adware
	C)	Troyan otlari.
	D)	Spyware
158		**“Foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod”. Bu xususiyat qaysi zararli dastur turiga xos.**
	A)	Spyware
	B)	Backdoors
	C)	Adware
	D)	Troyan otlari.
159		**“Biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi”. Bu xususiyat qaysi zararli dastur turiga xos.**
	A)	Mantiqiy bombalar
	B)	Backdoors
	C)	Adware
	D)	Troyan otlari.
160		**“Obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshi uchun hujumchi tomonidan foydalaniladi”. Bu xususiyat qaysi zararli dastur turiga**
	A)	Botnet
	B)	Backdoors
	C)	Adware
	D)	Troyan otlari.
161		**“Qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to amalga oshirilishini talab qiladi”. Bu xususiyat qaysi zararli dastur turiga xos.**
	A)	Ransomware
	B)	Backdoors
	C)	Adware
	D)	Troyan otlari.
162		**Umumiy tapmoqni ikki qismga: ichki va tashqi tapmokga ajapatuvchi himoya vosi bu?**
	A)	Tapmoklapapo ekpan
	B)	Antivirus
	C)	Virtual himoyalangan tarmoq
	D)	Router
163		**Paket filterlari turidagi tarmoqlararo ekran vositasi OSI modelining qaysi sath ishlaydi?**
	A)	Tarmoq sathida
	B)	Transport sathida
	C)	Ilova sathida
	D)	Kanal sathida

164		**Tashqi tapmokdagi foydalonuvchilapdan ichki tapmok pesupslapini ximoyalash q tarmoq himoya vositasining vazifasi hisoblanadi.**
	A)	Tapmoklapapo ekpan
	B)	Antivirus
	C)	Virtual himoyalangan tarmoq
	D)	Router
165		**Ichki tapmok foydalanuvchilapini tashqi tapmokqa bo‘lgan mupojaatla chegapalash qaysi tarmoq himoya vositasining vazifasi hisoblanadi.**
	A)	Tapmoklapapo ekpan
	B)	Antivirus
	C)	Virtual himoyalangan tarmoq
	D)	Router
166		**Qaysi tarmoq himoya vositasi tapmok manzili, identifikatoplap, intepfeys manzili, p nomepi va boshqa parametrlap yordamida filterlashni amalga oshiradi.**
	A)	Tapmoklapapo ekpan
	B)	Antivirus
	C)	Virtual himoyalangan tarmoq
	D)	Router
167		**Ikki uzel opasida axbopotni konfidensiyalligini va butunligini ta’minlash uchun himoyalangan tunelni quruvchi himoya vositasi bu?**
	A)	Virtual Private Network
	B)	Tapmoklapapo ekpan
	C)	Antivirus
	D)	Router
168		**Qaysi himoya vositasi tarmoqda uzatilayotgan axborotni butunligi, maxfiyligi va tomonlar autentifikatsiyasini ta’minlaydi?**
	A)	Virtual Private Network
	B)	Tapmoklapapo ekpan
	C)	Antivirus
	D)	Router
169		**Qaysi himoya vositasida mavjud paket shifplangan xolda yangi hosil qilingan mant paket ichiga kipitiladi?**
	A)	Virtual Private Network
	B)	Tapmoklapapo ekpan
	C)	Antivirus
	D)	Router
170		**Virtual xususiy tarmoq OSI modelining kanal sathida qaysi protokollar yordam amalga oshiriladi?**
	A)	L2F, L2TP
	B)	PPTP, TLS
	C)	TLS, TCP
	D)	L2TP, IP
171		**Virtual xususiy tarmoq OSI modelining tarmoq sathida qaysi protokol yordamida amalga oshiriladi?**
	A)	IPSec
	B)	L2TP
	C)	TCP
	D)	PPTP

172		**Virtual xususiy tarmoq OSI modelining seans sathida qaysi protokol yordamida amalga oshiriladi?**
	A)	TLS
	B)	L2TP
	C)	TCP
	D)	PPTP
173		**Ochiq tapmok yordamida ximoyalangan tapmokni qupish imkoniyatiga ega him vositasi bu?**
	A)	Virtual Private Network
	B)	Tapmoklapapo ekpan
	C)	Antivirus
	D)	Router
174		**“Mavjud bo‘lgan IP - paket to‘liq shifplanib, unga yangi IP saplavha bepiladi”. Ush amal qaysi himoya vositasi tomonidan amalga oshiriladi.**
	A)	Virtual Private Network
	B)	Tapmoklapapo ekpan
	C)	Antivirus
	D)	Router
175		**Foydalanuvchi tomonidan kiritilgan taqiqlangan so‘rovni qaysi himoya vosi yordamida nazoratlash mumkin.**
	A)	Tapmoklapapo ekpan
	B)	Virtual Private Network
	C)	Antivirus
	D)	Router
176		**Qaysi himoya vositasi tomonlarni autentifikatsiyalash vazifasini amalga oshiradi.**
	A)	Virtual Private Network
	B)	Tapmoklapapo ekpan
	C)	Antivirus
	D)	Router
177		**Qaysi himoya vositasi etkazilgan axbopotni butunligini va to‘g‘piligini tekshi vazifasini amalga oshiradi.**
	A)	Virtual Private Network
	B)	Tapmoklapapo ekpan
	C)	Antivirus
	D)	Router
178		**Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga imkon beruvchi himoya vo bu?**
	A)	Tapmoklapapo ekpan
	B)	Virtual Private Network
	C)	Antivirus
	D)	Router
179		**Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?**
	A)	Texnik vositalarning buzilishi va ishlamasligi
	B)	Axborotdan ruhsatsiz foydalanish
	C)	Zararkunanda dasturlar
	D)	An’anaviy josuslik va diversiya
180		**Axborotni deshifrlash deganda qanday jarayon tushuniladi?**

	A)	Yopiq axborotni kalit yordamida ochiq axborotga o‘zgartirish
	B)	Saqlanayotgan sirli ma’lumotlarni tarqatish
	C)	Tarmoqdagi ma’lumotlardan ruxsatsiz foydalanish
	D)	Tizim resurslariga noqonuniy ulanish va foydalanish
181		**Axborotni qanday ta’sirlardan himoyalash kerak?**
	A)	Axborotdan ruxsatsiz foydalanishdan, uni buzilishdan yoki yo‘q qilinishidan
	B)	Axborotdan qonuniy foydalanishdan, uni qayta ishlash yoki sotishdan
	C)	Axborotdan qonuniy foydalanishdan, uni qayta ishlash yoki foydalanishdan
	D)	Axborotdan tegishli foydalanishdan, uni tarmoqda uzatishdan
182		**Axborotni maxfiyligini ta’minlashda quyidagi algoritmlardan qaysilari foydalaniladi**
	A)	RSA, DES, AES
	B)	AES, CRC, SHA1
	C)	MD5, DES, ERI
	D)	ERI, MAC, SHA2
183		**Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?**
	A)	Ma’lumotlar butunligi
	B)	Axborotning konfidensialligi
	C)	Foydalanuvchanligi
	D)	Ixchamligi
184		**Axborotni foydalanuvchanligini buzushga qaratilgan tahdidni aniqlang.**
	A)	DDOS tahdidlar
	B)	Nusxalash tahdidlari
	C)	Modifikatsiyalash tahdidlari
	D)	O‘rtaga turgan odam tahdidi
185		**Axborotni shifrlash deganda qanday jarayon tushuniladi?**
	A)	Ochiq axborotni kalit yordamida yopiq axborotga o‘zgartirish
	B)	Kodlangan malumotlarni yig‘ish
	C)	Axborotlar o‘zgartirish jarayoni
	D)	Jarayonlar ketma-ketligi
186		**Virtual himoyalangan tunnelning asosiy afzalligi-bu?**
	A)	Tashqi faol va passiv kuzatuvchilarning foydalanishi juda qiyinligi
	B)	Tashqi faol va passiv kuzatuvchilarning foydalanishi juda oddiyligi
	C)	Tashqi faol va passiv kuzatuvchilarning foydalanishi juda qulayligi
	D)	Tashqi faol va passiv kuzatuvchilarning foydalanish imkoniyati ko‘pligi
187		**Global simsiz tarmoqning ta’sir doirasi qanday?**
	A)	Butun dunyo bo‘yicha
	B)	Binolar va korpuslar
	C)	O‘rtacha kattalikdagi shahar
	D)	Foydalanuvchi yaqinidagi tarmoq
188		**Dinamik parol-bu:**
	A)	Bir marta ishlatiladigan parol
	B)	Ko‘p marta ishlatiladigan parol
	C)	Foydalanuvchi ismi
	D)	Murakkab parol
189		**Eng ko‘p foydalaniladigan autentifikatsiyalash asosi-bu:**
	A)	Parolga asoslangan
	B)	Tokenga asoslangan

	C)	Biometrik parametrlarga asoslangan
	D)	Smart kartaga asoslangan
190		**Zararli dasturlarni ko‘rsating?**
	A)	Kompyuter viruslari va mantiqiy bombalar
	B)	Letsenziyasiz dasturlar va qurilmalar
	C)	Tarmoq kartasi va dasturlar
	D)	Internet tarmog‘i dasturlari
191		**RSA shifrlash algoritmida tanlangan p va q sonlarga qanday talab qo‘yiladi?**
	A)	Tub bo‘lishi
	B)	O‘zaro tub bo‘lishi
	C)	Butun son bo‘lishi
	D)	Toq son bo‘lishi
192		**12 soni bilan o‘zaro tub bo‘lgan sonlarni ko‘rsating?**
	A)	5,7,11
	B)	13,4,7
	C)	11,2,5
	D)	13,11,10
193		**Bluetooth standarti qaysi simsiz tarmoq turiga qiradi?**
	A)	Shaxsiy simsiz tarmoq
	B)	Lokal simsiz tarmoq
	C)	Mintaqaviy simsiz tarmoq
	D)	Global simsiz tarmoq
194		**Parolga “tuz”ni qo‘shib xeshlashdan maqsad?**
	A)	Tahdidchi ishini oshirish
	B)	Murakkab parol hosil qilish
	C)	Murakkab xesh qiymat hosil qilish
	D)	Ya’na bir maxfiy parametr kiritish
195		**Parol kalitdan nimasi bilan farq qiladi?**
	A)	Tasodifiylik darajasi bilan
	B)	Uzunligi bilan
	C)	Belgilari bilan
	D)	Samaradorligi bilan
196		**Kriptografik himoya axborotning quyidagi xususiyatlaridan qay birini ta’minlamaydi?**
	A)	Foydalanuvchanlikni
	B)	Butunlikni
	C)	Maxfiylikni
	D)	Autentifikatsiyani
197		**Elektron raqamli imzo tizimi foydalanuvchining elektron raqami imzosini uning im chekishdagi maxfiy kalitini bilmasdan qalbakilashtirish imkoniyati nimalarga bog‘l**
	A)	Buning imkoni yo‘q
	B)	Foydalanilgan matematik muammoga
	C)	Ochiq kalit uzunligiga
	D)	Imzo chekiladigan matnni konfidensialligiga
198		**Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni-bu:**
	A)	Identifikatsiya
	B)	Autentifikatsiya
	C)	Avtorizatsiya

	D)	Ma’murlash
199		**Sub’ektga ma’lum vakolat va resurslardan foydalanish imkoniyatini berish muolaj bu:**
	A)	Avtorizatsiya
	B)	Autentifikatsiya
	C)	Identifikatsiya
	D)	Haqiqiylikni ta’minlash
200		**Lokal simsiz tarmoqlarga tegishli texnologiyani ko‘rsating?**
	A)	WI-FI
	B)	WI-MAX
	C)	GSM
	D)	Bluetooth
201		**Qaysi shifrlash algoritmi GSM tarmog‘ida foydalaniladi?**
	A)	A5/1
	B)	RC4
	C)	AES
	D)	RSA
202		**Qaysi javobda elektron raqamli imzoning afzalligi noto‘g‘ri keltirilgan?**
	A)	Imzo chekilgan matn foydalanuvchanligini kafolatlaydi
	B)	Imzo chekilgan matn imzo qo‘yilgan shaxsga tegishli yekanligini tasdiqlaydi
	C)	Shaxsga imzo chekilgan matnga bog‘liq majburiyatlaridan tonish imkoniyatini bermaydi
	D)	Imzo chekilgan matn yaxlitligini kafolatlaydi
203		**Tomonlar autentifikatsiyasini, uzatilayotgan ma’lumot butunligi va maxfiyli ta’minlovchi himoya vositasi bu?**
	A)	VPN
	B)	Tarmoqlararo ekran
	C)	Antivirus
	D)	Router
204		**Paket filterlari turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni ama oshiradi?**
	A)	Tarmoq sathi parametrlari asosida
	B)	Kanal sathi parametrlari asosida
	C)	Ilova sathi parametrlari asosida
	D)	Taqdimot sathi parametrlari asosida
205		**OSI modelining qaysi sathida VPNni qurib bo‘lmaydi?**
	A)	Fizik sathda
	B)	Kanal sathda
	C)	Tarmoq sathda
	D)	Seans sathda
206		**Qaysi tarmoq himoya vositasi taqiqlangan saytlardan foydalanish imkoniyatini bera**
	A)	VPN
	B)	Tarmoqlararo ekran
	C)	Antivirus
	D)	Router
207		**OSI modelinining tarmoq sathiga mos parametrni ko‘rsating?**
	A)	IP manzil
	B)	MAS manzil
	C)	Portlar

	D)	SSL protokoli
208		**OSI modelining kanal sathiga mos parametrni ko‘rsating?**
	A)	MAS manzil
	B)	IP manzil
	C)	Portlar
	D)	SSL protokoli
209		**OSI modelining transport sathiga mos parametrni ko‘rsating?**
	A)	Portlar
	B)	MAS manzil
	C)	IP manzil
	D)	SSL protokoli
210		**Hodisalarni qayd etish quyidagilardan qaysi imkoniyatni taqdim etmaydi?**
	A)	Yo‘qolgan ma’lumotni tiklash imkoniyatini
	B)	Bo‘lishi mumkin bo‘lgan hujumni oldini olish imkoniyatini
	C)	Xatolik sababini bilish imkoniyatini
	D)	Holat haqida to‘liq ma’lumot olish imkoniyatini
211		
	A)	
	B)	
	C)	
	D)	
	A)	
	B)	
	C)	
	D)	
	A)	
	B)	
	C)	
	D)	
	A)	
	B)	
	C)	
	D)	
	A)	
	B)	
	C)	
	D)	
	A)	
	B)	
	C)	
	D)	
	A)	

	B)	
	C)	
	D)	
	A)	
	B)	
	C)	
	D)	
	A)	
	B)	
	C)	
	D)	
	A)	
	B)	
	C)	
	D)	
	A)	
	B)	
	C)	
	D)	
	A)	
	B)	
	C)	
	D)	