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

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

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

51	Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo'linadi?	Sust va faol
52	Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?	SMTP, POP yoki IMAR
53	Axborot resursi – bu?	axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi
54	Shaxsning, o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo'llaniladigan belgilar ketma-ketligi bo'lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu?	login
55	Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – bu?	parol
56	Identifikatsiya jarayoni qanday jarayon?	axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni
57	Autentifikatsiya jarayoni qanday jarayon?	ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
58	Avtorizatsiya jarayoni qanday jarayon?	foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
59	Ro'yxatdan o'tish bu?	foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
60	Axborot qanday sifatlarga ega bo'lishi kerak?	ishonchli, qimmatli va to'liq
61	Axborotning eng kichik o'lchov birligi nima?	bit
62	Elektronhujjatning rekvizitlari nechta qismdan iborat?	4
63	Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?	fleshka, CD va DVD disklar

64	Imzo bu nima ?	hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati.
65	Muhr bu nima?	hujjatning haqi-qiyligini va biror bir yuridik shaxsga tegishli ekanligi-ni tasdiqlovchi isbotdir.
66	DSA – nima	Raqamli imzo algoritmi
67	El Gamal algoritmi qanday algoritm	Shifrlash algoritmi va raqamli imzo algoritmi
68	Sezarning shifrlash sistemasining kamchiligi	Harflarning so’zlarda kelish chastotasini yashirmaydi
69	Axborot xavfsizligi va xavfsizlik san’ati haqidagi fan …. deyiladi?	Kriptografiya
70	Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu -	steganografiya
71	Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?	Deshifrlash
72	…… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.	Kiberxavfsizlik
73	Risk	Potensial foyda yoki zarar
74	Kiberxavfsizlik nechta bilim soxasini o‘z ichiga oladi.	8
75	“Ma’lumotlar xavfsizligi” bilim sohasi.....	ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.
76	“Dasturiy ta’minotlar xavfsizligi” bilim sohasi.....	foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.
77	“Tashkil etuvchilar xavfsizligi”	katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.
78	“Aloqa xavfsizligi” bilim sohasi.....	tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

79	“Tizim xavfsizligi” bilim sohasi……	tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi.
80	“Inson xavfsizligi” bilim sohasi….	kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.
81	“Tashkilot xavfsizligi” bilim sohasi ….	tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini
82	“Jamoat xavfsizligi” bilim sohasi …..	u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi.
83	Tahdid nima? tizim yoki	Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.
84	Kodlash nima?	Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir
85	Shifrlash nima?	Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi
86	Bir martalik bloknotda Qanday kalitlardan foydalaniladi?	Ochiq kalitdan
87	Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing.	23
88	Agar RSA algotirmida n ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.	$M = C^d \bmod n$;
89	O’nlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq tizi miga o’tkazing. 65	100001
90	Quyidagi modulli ifodani qiymatini toping. (125*45)mod10.	5
91	Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256.	244

92	Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.	$C = M^e \bmod n$; -tog'ri javob
93	Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug'ullanadi	Kriptologiya.
94	Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi	$\{d, n\}$ – yopiq, $\{e, n\}$ – ochiq;
95	Zamonaviy kriptografiya qanday bo'limlardan iborat?	Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish
96	1. Kriptografik usullardan foydalanishning asosiy yo'nalishlari nimalardan iborat?	Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarni haqiqiyligini aniqlash, tashuvchilarda axborotlarni shifrlangan ko'rinishda saqlash (masalan, hujjatlarni, ma'lumotlar bazasini)
97	Shifr nima?	Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan krptografik algoritm
98	Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?	Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi
99	Oqimli shifrlashning mohiyati nimada?	Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma'lumotlarnbi bitlar yoki belgilar bo'yicha shifrlaydi

100	Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating.	uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim,
101	Kriptotizim quyidagi komponentlardan iborat:	ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, Ek : M $\rightarrow$ C (shifrlash uchun) va Dk: C$\rightarrow$M (deshifrlash uchun) funktsiyalar
102	Serpent, Square, Twofish, RC6 , AES algoritmlari qaysi turiga mansub?	simmetrik blokli algoritmlar
103	DES algoritmiga muqobil bo’lgan algoritmni ko’rsating.	Uch karrali DES, IDEA, Rijndael
104	DES algoritmining asosiy muammosi nimada?	kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas
105	Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?	shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun
106	12+22 mod 32 ?	2
107	2+5 mod32 ?	7
108	Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi.	ochiq kalitlar
109	12+11 mod 16 ?	7
110	RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo’llab quvvatlaydi.	128 bitli, 192 bitli, 256 bitli
111	Xesh-funktsiyani natijasi …	uzunlikdagi xabar
112	RSA algoritmi qanday jarayonlardan tashkil topgan	Kalitni generatsiyalash; Shifrlash; Deshifrlash.
113	RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida necha bit bo‘lishi talab etiladi.	2048
114	Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi	Xesh funksiyalar
115	To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub	Xalqa

116	Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo’llamasligi mumkin	to’liq bog’lanishli
117	Kompyuterning tashqi interfeysi deganda nima tushuniladi	kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari
118	Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi	Yulduz
119	Ethernet kontsentratori qanday vazifani bajaradi	kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi
120	OSI modelida nechta sath mavjud	7
121	OSI modelining to’rtinchi sathi qanday nomlanadi	Transport sathi
122	OSI modelining beshinchi sathi qanday nomlanadi	Seanslar sathi
123	OSI modelining birinchi sathi qanday nomlanadi	Fizik sath
124	OSI modelining ikkinchi sathi qanday nomlanadi	Kanal sathi
125	OSI modelining uchinchi sathi qanday nomlanadi	Tarmoq sathi
126	OSI modelining oltinchi sathi qanday nomlanadi	Taqdimlash sathi
127	OSI modelining ettinchi sathi qanday nomlanadi	Amaliy sath
128	OSI modelining qaysi sathlari tarmoqqa bog’liq sathlar hisoblanadi	fizik, kanal va tarmoq sathlari
129	OSI modelining tarmoq sathi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi	Marshrutizator
130	Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi	Fizik sath
131	Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi sathi bajaradi	Tarmoq sathi
132	Keltirilgan protokollarning qaysilari tarmoq sathi protokollariga mansub	IP, IPX
133	Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub	TCP,UDP
134	OSI modelining fizik sathi qanday funktsiyalarni bajaradi	Elektr signallarini uzatish va qabul qilish
135	OSI modeliningamaliy sathi qanday funktsiyalarni bajaradi	Klient dasturlari bilan o’zaro muloqotda bo’lish
136	Keltirilgan protokollarning qaysilari kanal sathi protokollariga mansub	Ethernet, FDDI
137	Keltirilgan protokollarning qaysilari taqdimlash sathi protokollariga mansub	SNMP, Telnet
138	Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...	Avtorizatsiya
139	Autentifikatsiya faktorlari nechta	3

140	Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima	Parol
141	Ko‘z pardasi, yuz tuzilishi, ovoz tembri.	Biometrik autentifikatsiya
142	barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi.	Fizik satx
143	Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi	2
144	Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi.	Foydalanishni boshqarish
145	Foydalanishni boshqarish –bu...	sub’ektni sub’ektga ishlash qobilyatini aniqlashdir.
146	Foydalanishna boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi,	Sub’ekt
147	Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ?	Ob’ekt
148	Foydalanishna boshqarishning nechta usuli mavjud?	4
149	Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy ob’ektlarni himoyalash uchun qo‘llaniladi	DAC
150	Foydalanishni boshqarishning qaysi modelida ob’ekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi	DAC
151	Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi.	MAC
152	Foydalanishni boshqarishning mandatli modelida Ob’ektning xavfsizlik darajasi nimaga bog‘liq..	Tashkilotda ob’ektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi
153	MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi	xavfsizlik siyosati ma’muri
154	Agar sub’ektning xavfsizlik darajasida ob’ektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi	O‘qish
155	Agar sub’ektning xavfsizlik darajasi ob’ektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.	Yozish

156	Foydalanishni boshqarishning qaysi modelida har bir ob’ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun ob’ektlardan foydalanish ruxsati ko‘rsatiladi?	RBAC
157	Rol tushunchasiga ta’rif bering.	Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin
158	Foydalanishni boshqarishning qaysi usuli - ob’ektlar va sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.	ABAC
159	XACML foydalanishni boshqarishni qaysi usulining standarti?	ABAC
160	Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?	barchasi
161	Axborotning kriptografik himoya vositalari necha turda?	3
162	Dasturiy shifrlash vositalari necha turga bo‘linadi	4
163	Diskni shifrlash nima uchun amalga oshiriladi?	Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
164	Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?	4
165	Kompyuter tarmoqlari bu –	Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi
166	Tarmoq modeli –bu.. ikki	Hisoblash tizimlariorasidagi aloqani ularning ichki tuzilmaviy vatexnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir to‘plami
167	OSI modelida nechta tarmoq sathi bor	7
168	OSI modeli 7 stahi bu	Ilova
169	OSI modeli 1 stahi bu	Fizik
170	OSI modeli 2 stahi bu	Kanal
171	TCP/IP modelida nechta satx mavjud	4
172	Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi.	Shaxsiy tarmoq

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

188	Tarmoq modeli-bu...	Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir
189	OSI modeli nechta sathga ajraladi?	7
190	Fizik sathning vazifasi nimadan iborat	Qurilma, signal va binar o‘zgartirishlar
191	Ilova sathning vazifasi nimadan iborat	Ilovalarni tarmoqqa ulanish jarayoni
192	Kanal sathning vazifasi nimadan iborat	Fizik manzillash
193	Tarmoq sathning vazifasi nimadan iborat	Yo‘lni aniqlash va mantiqiy manzillash
194	TCP/IP modeli nechta sathdan iborat	4
195	Quyidagilarninf qaysi biri Kanal sathi protokollari	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35.
196	Quyidagilarninf qaysi biri tarmoq sathi protokollari	. IP, ICMP, ARP, RARP
197	Quyidagilarninf qaysi biri transport sathi protokollari	TCP, UDP, RTP
198	Quyidagilarninf qaysi biri ilova sathi protokollari	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP va hak
199	TCP/IP modelining kanal sathiga OSI modelining qaysi sathlari mos keladi	Kanal, Fizik
200	TCP/IP modelining tarmoq sathiga OSI modelining qaysi sathlari mos keladi	Tarmoq
201	TCP/IP modelining transport sathiga OSI modelining qaysi sathlari mos keladi	Tramsport
202	TCP/IP modelining ilova sathiga OSI modelining qaysi sathlari mos keladi	Ilova, taqdimot, seans
203	Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.	Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
204	Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.	. Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
205	Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang.	Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi

206	Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang.	Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi
207	Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan	Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi
208	Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan	Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi
209	Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan	Yuboriluvchi va qabul qilinuvchi ma’lumot TOKYeN yordamida manziliga yetkaziladi
210	Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan	Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi
211	Tarmoq kartasi nima?	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
212	Repetir nima?	Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
213	Hub nima?	Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
214	Switch nima?	Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
215	Router nima?	Qabul qilingan ma’lumotlarni tarmoq sathiga tegishli manzillarga ko‘ra (IP manzil) uzatadi
216	DNS tizimlari.	Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi
217	TCP bu- …	Transmission Control Protocol
218	UDP bu-…	User datagram protocol

219	Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang	Ichki, tashqi
220	Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi	Biznes jarayonlarni to‘xtab qolishiga olib keladi
221	Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi	Hujum natijasida ishlab chiqarishi yo‘qolgan hollarda uni qayta tiklash ko‘p vaqt talab qiladi va bu vaqtda ishlab chiqarish to‘xtab qoladi
222	Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi	Konfidensial axborotni chiqib ketishi natijasida, tashkilot shaxsiy ma’lumotlarini yo‘qolishi mumkin
223	Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi	Tashkilot xodimlarining shaxsiy va ishga oid ma’ulmotlarini kutilmaganda oshkor bo‘lishi ushbu xodimlarga bevosita ta’sir qiladi
224	Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi	Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi
225	Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi	tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi
226	Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi.	Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.
227	Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi	Razvedka hujumlari
228	Ma’lumotlarni zaxira nusxalash bu – …	Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi
229	Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz	Zaxira nusxalash

230	Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering	Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
231	Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi?	5
232	Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi.	4
233	Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash	Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart.
234	RAID texnologiyasining transkripsiyasi qanday.	Random Array of Independent Disks
235	RAID texnologiyasida nechta satx mavjud	6
236	OSI modelining birinchi sathi qanday nomlanadi	Fizik sath
237	OSI modelining ikkinchi sathi qanday nomlanadi	Kanal sathi
238	OSI modelining uchinchi sathi qanday nomlanadi	Tarmoq sathi
239	OSI modelining oltinchi sathi qanday nomlanadi	Taqdimlash sathi
240	OSI modelining ettinchi sathi qanday nomlanadi	Amaliy sath
241	Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi	Fizik sath
242	Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub	TCP,UDP
243	OSI modelining fizik sathi qanday funktsiyalarni bajaradi	Elektr signallarini uzatish va qabul qilish
244	OSI modelining amaliy sathi qanday funktsiyalarni bajaradi	Klient dasturlari bilan o’zaro muloqotda bo’lish
245	12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan sonlar soni nechta?	8 ta
246	Yevklid algoritmi qanday natijani beradi?	Sonning eng katta umumiy bo’luvchisini toppish

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

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

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

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

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

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

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

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

352	Lampsonning foydalanishni boshqarish matritsasi nimalardan tashkil topgan?	Imtiyozlar ro'yxati
353	Access control list va Capability list bu nimaning asosiy elementi xisoblanadi?	Lampson matritsasining
354	Lampson matritsasining satrlarida nima ifodalanadi?	Sub'ektlar
355	Foydalanishni boshqarishning mantiqiy vositalari infratuzilma va uning ichidagi tizimlarda ... uchun foydalaniladi.	Mandat, Tasdiqlash, Avtorizatsiya
356	SHaxsiy simsiz tarmoq standartini aniqlang.	Bluetooth, IEEE 802.15, IRDA
357	Lokal simsiz tarmoq standartini aniqlang.	IEEE 802.11, Wi-Fi, HiperLAN
358	Regional simsiz tarmoq standartini aniqlang.	IEEE 802.16, WiMAX
359	Global simsiz tarmoq standartini aniqlang.	CDPD, 2G, 2.5G, 3G, 4G, 5G
360	Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang.	SHaxsiy simsiz tarmoq
361	IEEE 802.11, Wi-Fi, HiperLAN standartida ishlovchi simsiz tarmoq turini aniqlang.	Lokal simsiz tarmoq
362	IEEE 802.16, WiMAX standartida ishlovchi simsiz tarmoq turini aniqlang.	Regional simsiz tarmoq
363	CDPD, 2G, 2.5G, 3G, 4G, 5G standartida ishlovchi simsiz tarmoq turini aniqlang.	Global simsiz tarmoq
364	Bluetooth qanday chastota oralig'ida ishlaydi?	2.4-2.485 Ggts
365	Wi-Fi qanday chastota oralig'ida ishlaydi?	2.4-5 Ggts
366	WiMax tarmog'ining tezligi qancha?	1 Gbit/sekund
367	Quyidagilardan qaysi biri MITM xujumiga tegishli xatti-xarakat ximoblanadi?	Aloqa seansini konfidentsialligini va yaxlitligini buzish
368	WiMAX tarmoq arxitekturasi nechta tashkil etuvchidan iborat?	5
369	WiMAX tarmoq arxitekturasi qaysi tashkil etuvchidan iborat?	Base station, Subscriber station, Mobile station, Relay station, Operator network
370	GSM raqamli mobil telefonlarining nechanchi avlodi uchun ishlab chiqilgan protokol?	Ikkinchi avlodi
371	GSM standarti qaysi tashkilot tomonidan ishlab chiqilgan?	European telecommunications standards institute
372	.... – o'zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma'lumoti va xavfsizlik algoritmlarini saqlaydi.	Sim karta
373	Rutoken S qurilmasining og'irligi qancha?	6.3 gramm
374	True Crypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?	AES, Serpent, Twofish

375	Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidentsialligini aniqlash qaysi dasturiy shifrlash vositalarining vazifasi?	Disc encryption software
376	BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?	AES, Serpent, Twofish
377	AxCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?	AES-256
378	Qog’oz ko’rinishidagi axborotlarni yo’q qilish qurilmasining nomini kiriting.	Shreder
379	Ma’lumotlarni bloklarga bo’lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?	RAID 0
380	Qaysi texnologiyada ma’lumotni ko’plab nusxalari bir vaqtda bir necha disklarga yoziladi?	RAID 1
381	Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi?	RAID 3
382	Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?	RAID 5
383	Disk zararlanganda “qaynoq almashtirish” yordamida uni almashtirish mumkin. Bu xususiyat qaysi texnologiyaga tegishli?	RAID 50
384	Zaxiralashning qanday turlari mavjud?	To’liq, o’sib boruvchi, differentsial
385	IOS, Android, USB xotiralardan ma’lumotlarni tiklash uchun qaysi dasturdan foydalaniladi?	EASEUS Data recovery wizard
386	Foydalanuvchi ma’lumotlarini qo’lga kirituvchi va uni xujumchiga yuboruvchi dasturiy kod nima?	Spyware
387	Operatsion tizim tomonidan aniqlanmasligi uchun ma’lum xarakatlarni yashirish nima deyiladi?	Rootkits
388	Qurbon kompyuterda mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo’yib to’lov amalga oshirishni talab qiladi. Bu qaysi zararli dastur?	Ransomware
389	Quyidagilardan o’zidan ko’payishi yo’q bo’lganlarini belgilang.	Mantiqiy bomba, Troyan oti, Backdoors
390	Viruslar resurslardan foydalanish usuliga ko’ra qanday turlarga bo’linadi?	Virus parazitlar, virus chervlar
391	Viruslar zararlangan ob’ektlar turiga ko’ra qanday turlarga bo’linadi?	Dasturiy, yuklanuvchi, makroviruslar, ko’p platformali
392	Viruslar faollashish printsipiga ko’ra qanday turlarga bo’linadi?	Rezident, norezident
393	Viruslar dastur kodini tashkil qilish yondoshuviga ko’ra qanday turlarga bo’linadi?	SHifrlangan, shifrlanmagan, polimorf
394	Dastlabki virus nechanchi yilda yaratilgan?	1988

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

Xato

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

Paranoid siyosat

Zaxiralashning qanday turlari mavjud?

Ichki, tashqi

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

Hakker

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

Axborot tizimlari

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

RAID 0

Spam bilan kurashishning dasturiy uslubida nimalar ko‘zda tutiladi?

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

Botnet-nima?

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

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

RAID 5

Zararli dasturlar qanday turlarga bo‘linadi?

Tabiiy dasturlar va suniy dasturlar

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

Davlat va nodavlat tashkilotlari me’yorlarni

Ma’lumotlarni zaxira nusxalash bu – …

Ma'lumotlar xavfsizligini ta'minlash uchun qo‘llaniladigan shifrlash jarayoni

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

Global tarmoqdan uzib qo‘yish

Dastlabki virus nechanchi yilda yaratilgan?

1988

System-Specific SecurityPolicies, SSSP-bu…

Muammoga qaratilgan xavfsizlik siyosati

Enterprise Information Security Policies, EISP-bu…

Tizimga qaratilgan xavfizlik siyosati

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

"To‘liq zaxiralash"

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

O‘ta maxfiy, maxfiy

TO’G’RILARI:

OSI modelida nechta tarmoq satxi bor ?
J: 7
OSI modelining birinchi satxi qanday nomlanadi
J: Fizik satx
OSI modelining ikkinchi satxi qanday nomlanadi
J: Kanal satxi
OSI modelining uchinchi satxi qanday nomlanadi
J: Tarmoq satxi
OSI modelining oltinchi satxi qanday nomlanadi
J: Taqdimlash satxi
OSI modelining yettinchi satxi qanday nomlanadi
J: Amaliy satx
OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi
J: fizik, kanal va tarmoq satxlari
OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi
J: Marshrutizator
OSI modelining fizik satxi qanday funktsiyalarni bajaradi
J: Elektr signallarini uzatish va qabul qilish
Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ?
J: Obyekt
Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?
J: Subyekt
Simmetrik kriptotizimlarda ... jumlani davom ettiring
J: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi
Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.
J: 2 turga
Axborotning eng kichik o’lchov birligi nima?
J: bit
Ko‘z pardasi, yuz tuzilishi, ovoz tembri-: bular autentifikatsiyaning qaysi faktoriga mos belgilar?
J: Biometrik autentifikatsiya
Kriptografiyaning asosiy maqsadi...
J: maxfiylik, yaxlitlilikni ta`minlash
Ro’yxatdan o’tish bu?
foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
Qanday xujumda zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi?
J: Zararli hujumlar
Qanday xujumda hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi?
J: Kirish hujumlari
Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub
J: Ethernet, FDDI
Xesh-:funktsiyani natijasi …
J: fiksirlangan uzunlikdagi xabar
Ethernet kontsentratori qanday vazifani bajaradi
J: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi
Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?
J: fleshka, CD va DVD disklar
Faol hujum turi deb…
J: Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon

Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi.
J: MAC
Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo‘llaniladi
J: DAC
Foydalanishni boshqarishning qaysi modelida Obyekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi
J: DACfInternetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?
Foydalanishni boshqarishning qaysi usuli -: Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.
J: ABAC
Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun Obyektlardan foydalanish ruxsati ko‘rsatiladi?
J: RBAC
To’rtta bir-:biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub
J: Xalqa Yulduz To’liq bog’lanishli Yacheykali
Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi?
J: DNS tizimlari, Razvedka hujumlari
…… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.
J: Kiberxavfsizlik
Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?
J: raqamli imzoni shakllantirish va tekshirish muolajasi
Kriptologiya -:
J: axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?
J: Deshifrlash
Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.
J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik
Autentifikatsiya faktorlari nechta
J: 3
Kriptografiyada matn –
J: alifbo elementlarining tartiblangan to’plami
Konfidentsiallikga to’g’ri ta`rif keltiring.
J: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-:ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu?
J: login
Kriptoanaliz –
J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
sifatlarga ega bo’lishi kerak?
J: ishonchli, qimmatli va to’liq
Shifrlash –
J: akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi
Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?

J: simmetrik kriptosistemalar
Foydalanishni boshqarish –bu...
J: Subyektni Obyektga ishlash qobilyatini aniqlashdir.
Kompyuterning tashqi interfeysi deganda nima tushuniladi?
J: kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidalari to'plamlari
Kodlash nima?
J: Ma'lumotni osongina qaytarish uchun hammaga
Tarmoq kartasi bu...
J: Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
Elektron raqamli imzo deb –
J: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo'shilgan qo'shimcha
Hab bu...
J: ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi.
Switch bu...
J: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
Axborot xavfsizligining asosiy maqsadlaridan biri-: bu…
J: Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish
Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-:ketligi (maxfiy so'z) – bu?
J: parol
Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?
J: SMTP, POP yoki IMAR
Kalit taqsimlashda ko'proq nimalarga e`tibor beriladi?
J: Tez, aniq va maxfiyligiga
Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi.
J: Yozish
Qanday xujumda hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi?
J: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
Kalit – bu …
J: Matnni shifrlash va shifrini ochish uchun kerakli axborot
Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
J: Fizik satx
Blokli shifrlash-:
J: shifrlanadigan matn blokiga qo'llaniladigan asosiy akslantirish
Kriptobardoshlilik deb …
J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
Ma'lumotlar butunligi qanday algritmlar orqali amalga oshiriladi
J: Xesh funksiyalar
Kriptografiya –
J: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
J: TCP,UDP
Tekstni boshqa tekst ichida ma'nosini yashirib keltirish bu -:
J: steganografiya
Yaxlitlikni buzilishi bu -: …
J: Soxtalashtirish va o'zgartirish

Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?
J: barchasi
Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub
J: Ethernet, FDDI
Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?
J: Foydalanishni boshqarish
Tarmoq repiteri bu…
J: Signalni tiklash yoki qaytarish uchun foydalaniladi.
Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?
J: Ochiq kalitli kriptotizimlarda bir-:biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi
Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi
J: O‘qish
MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi
J: xavfsizlik siyosati ma’muri
Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?
J: Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi
Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi
J: Tarmoq satxi
Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bog‘liq..
J: Tashkilotda Obyektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi
Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi
J: {d, n} – yopiq, {e, n} – ochiq;
Diskni shifrlash nima uchun amalga oshiriladi?
J: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
Tahdid nima?
J: Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.
Risk
J: Potensial foyda yoki zarar
barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi?
J: Fizik satx
Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...
J: Avtorizatsiya
Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.
J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik
Kompyuter tarmoqlari bu –
J: Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan
Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?
J: raqamli imzoni shakllantirish va tekshirish muolajasi
Kriptografiyada matn –
J: alifbo elementlarining tartiblangan to’plami

Autentifikatsiya jarayoni qanday jarayon?
J: obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
Rol tushunchasiga ta’rif bering.
J: Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin
Avtorizatsiya jarayoni qanday jarayon?
J: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima
J: Parol
Elektron raqamli imzo deb –
J: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
TCP/IP modelida nechta satx mavjud
J: 4
Kriptoanaliz –
J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi?
J: Simmetrik va assimetrik
Shifrlash nima?
J: Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi
Kriptografiyada alifbo –
J: axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
Kripto tizimga qo’yiladigan umumiy talablardan biri
J: shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak
Simmetrik kriptotizmning uzluksiz tizimida …
J: ochiq matnning har bir harfi va simvoli alohida shifrlanadi
Axborot resursi – bu?
J: axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi
Stenografiya ma’nosi...
J: sirli yozuv
Identifikatsiya jarayoni qanday jarayon?
J: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.
J: Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
2. Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq?
J:simmetrik kriptotizimlar
3. Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.
J:Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
4. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?
J: parol
5. Rol tushunchasiga ta’rif bering.
Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin
6. Foydalanish huquqini cheklovchi matritsa modeli bu...
J:Bella La-Padulla modeli

8. Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?
J: Deshifrlash
9. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?
J:Strukturalarni ruxsatsiz modifikatsiyalash
10. Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi?
J:Kriptobardoshlik
11. Foydalanishni boshqarish –bu...
J: Sub’ektni Ob’ektga ishlash qobilyatini aniqlashdir.
12. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?
J: Yulduz
13. RSA algoritm qaysi yilda ishlab chiqilgan?
J: 1977 yil
14. Elektron xujjatlarni yo‘q qilish usullari qaysilar?
J:Shredirlash, magnitsizlantirish, yanchish
15. Kriptografiyada kalitning vazifasi nima?
J: Matnni shifrlash va shifrini ochish uchun kerakli axborot
16. WiMAX qanday simsiz tarmoq turiga kiradi?
J: Regional
17. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining maxfiy bo‘lmagan qayd yozuvi – bu…
J: login
18. Stenografiya ma’nosi qanday?
J: sirli yozuv
19. Fire Wall ning vazifasi...
J: Tarmoqlar orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta’minlaydi
20. Yaxlitlikni buzilishi bu - …
J: Soxtalashtirish va o‘zgartirish

1. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko‘rsating?
   DDoS (Distributed Denial of Service) hujum
2. Rezident virus…
   tezkor xotirada saqlanadi
3. Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyoti fanda qanday nomladi?
   AKT xavfsizlik siyosati
4. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.
   Recuva, R.saver
5. Zaiflik – bu…
   tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.
6. Axborot xavfsizligi timsollarini ko‘rsating.
   Alisa, Bob, Eva

7. Kiberetika tushunchasi:
   Kompyuter va kompyuter tarmoqlarida odamlarning etikasi
8. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuni qachon kuchga kirgan?
   1997 yil 24 aprel
9. DIR viruslari nimani zararlaydi?
   FAT tarkibini zararlaydi
10. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?
   Detektorlar
11. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?
   "Issiq zaxiralash"
12. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...
   Tamoqlararo ekranlarning o‘rnatilishi
13. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?
   Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan
14. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…
   Kiberjinoyat deb ataladi
15. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud?
   detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar
16. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?
   Ruxsat berishga asoslangan siyosat
17. DIR viruslari nimani zararlaydi?
   FAT tarkibini zararlaydi
18. Makroviruslar nimalarni zararlaydi?
   Ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.
19. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.
   HandyBakcup
20. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.
   "Sovuq saxiralash"
21. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.
   Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir
22. Polimorf viruslar tushunchasi to‘g‘ri ko‘rsating.
   Viruslar turli ko‘rinishdagi shifrlangan viruslar bo‘lib, o‘zining ikkilik shaklini nusxadan-nusxaga o‘zgartirib boradi
23. Fishing (ing. Phishing – baliq ovlash) bu…

Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

24.	Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.	Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik
25.	Axborot xavfsizligining asosiy maqsadlaridan biri-bu…	Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish
26.	Konfidentsiallikga to’g’ri ta`rif keltiring.	axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
27.	Yaxlitlikni buzilishi bu - …	Soxtalashtirish va o’zgartirish
28.	... axborotni himoyalash tizimi deyiladi.	Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi
29.	Kompyuter virusi nima?	maxsus yozilgan va zararli dastur
30.	Axborotni himoyalash uchun ... usullari qo’llaniladi.	kodlashtirish, kriptografiya, stegonografiya
31.	Stenografiya mahnosi...	sirli yozuv
32.	Kriptologiya yo’nalishlari nechta?	2
33.	Kriptografiyaning asosiy maqsadi...	maxfiylik, yaxlitlilikni ta`minlash
34.	SMTP - Simple Mail Transfer protokol nima?	elektron pochta protokoli
35.	SKIP protokoli...	Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi
36.	Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar…	uzilish, tutib qolish, o’zgartirish, soxtalashtirish
37.	...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.	konfidentsiallik
38.	Foydalanish huquqini cheklovchi matritsa modeli bu...	Bella La-Padulla modeli
39.	Kommunikatsion qism tizimlarida xavfsizlikni ta`minlanishida necha xil shifrlash ishlatiladi?	2
40.	Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi?	TCP/IP, X.25 protokollar
41.	Himoya tizimi kompleksligiga nimalar orqali erishiladi?	Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali
42.	Kalit – bu …	Matnni shifrlash va shifrini ochish uchun kerakli axborot
43.	Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?	simmetrik kriptotizimlar
44.	Autentifikatsiya nima?	Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi
45.	Identifikatsiya bu- …	Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni
46.	O’rin almashtirish shifri bu - …	Murakkab bo’lmagan kriptografik akslantirish
47.	Simmetrik kalitli shifrlash tizimi necha turga	2 turga

	bo’linadi.	
48.	Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular …	hosil qilish, yig’ish, taqsimlash
49.	Kriptologiya -	axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
50.	Kriptografiyada alifbo –	axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
51.	Simmetrik kriptotizimlarda ... jumlani davom ettiring	shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi
52.	Kriptobardoshlilik deb …	kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
53.	Elektron raqamli imzo deb –	xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
54.	Kriptografiya –	axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
55.	Kriptografiyada matn –	alifbo elementlarining tartiblangan to’plami
56.	Kriptoanaliz –	kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
57.	Shifrlash –	akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi
58.	Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi?	Tez, aniq va maxfiyligiga
59.	Faol hujum turi deb…	Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon
60.	Blokli shifrlash-	shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish
61.	Simmetrik kriptotizmning uzluksiz tizimida …	ochiq matnning har bir harfi va simvoli alohida shifrlanadi
62.	Kripto tizimga qo’yiladigan umumiy talablardan biri	shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak
63.	Quyidagi tengliklardan qaysilari shifrlash va deshifrlashni ifodalaydi?	Ek1(T)=T, Dk2(T1)=T
64.	Berilgan ta`riflardan qaysi biri assimmetrik tizimlarga xos?	Assimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi
65.	Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang	Vijiner matritsasi, Sezar usuli
66.	Akslantirish tushunchasi deb nimaga aytiladi?	1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga
67.	Simmetrik guruh deb nimaga aytiladi?	O’rin almashtirish va joylashtirish
68.	Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?	simmetrik kriptositemalar
69.	Xavfli viruslar bu - …	kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar
70.	Mantiqiy bomba – bu …	Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari

71.	Elektron raqamli imzo tizimi qanday muolajani amalga oshiradi?	raqamli imzoni shakllantirish va tekshirish muolajasi
72.	Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi?	Simmetrik va assimetrik
73.	Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?	Korporativ va umumfoydalanuvchi
74.	Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo'linadi?	Sust va faol
75.	Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?	SMTP, POP yoki IMAR
76.	Axborot resursi – bu?	axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi
77.	Shaxsning, o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo'llaniladigan belgilar ketma-ketligi bo'lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu?	login
78.	Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – bu?	parol
79.	Identifikatsiya jarayoni qanday jarayon?	axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni
80.	Autentifikatsiya jarayoni qanday jarayon?	ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
81.	Avtorizatsiya jarayoni qanday jarayon?	foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
82.	Ro'yxatdan o'tish bu?	foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
83.	Axborot qanday sifatlarga ega bo'lishi kerak?	ishonchli, qimmatli va to'liq
84.	Axborotning eng kichik o'lchov birligi nima?	bit
85.	Elektronhujjatning rekvizitlari nechta qismdan iborat?	4
86.	Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?	fleshka, CD va DVD disklar
87.	Imzo bu nima ?	hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati.
88.	Muhr bu nima?	hujjatning haqi-qiyligini va biror bir yuridik shaxsga tegishli ekanligi-ni tasdiqlovchi isbotdir.
89.	DSA – nima	Raqamli imzo algoritmi
90.	El Gamal algoritmi qanday algoritm	Shifrlash algoritmi va raqamli imzo algoritmi

91.	Sezarning shifrlash sistemasining kamchiligi	Harflarning so’zlarda kelish chastotasini yashirmaydi
92.	Axborot xavfsizligi va xavfsizlik san’ati haqidagi fan …. deyiladi?	Kriptografiya
93.	Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu -	steganografiya
94.	Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?	Deshifrlash
95.	…… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.	Kiberxavfsizlik
96.	Risk	Potensial foyda yoki zarar
97.	Kiberxavfsizlik nechta bilim soxasini o‘z ichiga oladi.	8
98.	“Ma’lumotlar xavfsizligi” bilim sohasi.....	ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.
99.	“Dasturiy ta’minotlar xavfsizligi” bilim sohasi.....	foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.
100.	“Tashkil etuvchilar xavfsizligi”	katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.
101.	“Aloqa xavfsizligi” bilim sohasi.....	tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.
102.	“Tizim xavfsizligi” bilim sohasi……	tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi.
103.	“Inson xavfsizligi” bilim sohasi….	kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi.
104.	“Tashkilot xavfsizligi” bilim sohasi ….	tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini
105.	“Jamoat xavfsizligi” bilim sohasi …..	u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi.
106.	Tahdid nima? tizim yoki	Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.
107.	Kodlash nima?	Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir
108.	Shifrlash nima?	Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi
109.	Bir martalik bloknotda Qanday kalitlardan	Ochiq kalitdan

	foydalaniladi?	
110.	Ikkilik sanoq tizimida berilgan 10111 sonini o'nlik sanoq tizimiga o'tkazing.	23
111.	Agar RSA algotirmida n ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.	$M = C^d \bmod n$;
112.	O'nlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq tizi miga o'tkazing. 65	100001
113.	Quyidagi modulli ifodani qiymatini toping. (125*45)mod10.	5
114.	Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256.	244
115.	Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.	$C = M^e \bmod n$; -tog'ri javob
116.	Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug'ullanadi	Kriptologiya.
117.	Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi	$\{d, n\}$ – yopiq, $\{e, n\}$ – ochiq;
118.	Zamonaviy kriptografiya qanday bo'limlardan iborat?	Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish
119.	1. Kriptografik usullardan foydalanishning asosiy yo'nalishlari nimalardan iborat?	Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarni haqiqiyligini aniqlash, tashuvchilarda axborotlarni shifrlangan ko'rinishda saqlash (masalan, hujjatlarni, ma'lumotlar bazasini)
120.	Shifr nima?	Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan krptografik algoritm
121.	Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?	Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi
122.	Oqimli shifrlashning mohiyati nimada?	Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma'lumotlarnbi bitlar yoki belgilar bo'yicha shifrlaydi
123.	Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating.	uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmasligi uchun algoritm yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog'liq bo'lishi lozim,
124.	Kriptotizim quyidagi komponentlardan iborat:	ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, Ek : M ® C (shifrlash uchun) va Dk: C®M (deshifrlash uchun) funktsiyalar

125.	Serpent, Square, Twofish, RC6 , AES algoritmlari qaysi turiga mansub?	simmetrik blokli algoritmlar
126.	DES algoritmiga muqobil bo'lgan algoritmni ko'rsating.	Uch karrali DES, IDEA, Rijndael
127.	DES algoritmining asosiy muammosi nimada?	kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas
128.	Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?	shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun
129.	12+22 mod 32 ?	2
130.	2+5 mod32 ?	7
131.	Kriptografik elektron raqamli imzolarda qaysi kalitlar ma'lumotni yaxlitligini ta'minlashda ishlatiladi.	ochiq kalitlar
132.	12+11 mod 16 ?	7
133.	RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo'llab quvvatlaydi.	128 bitli, 192 bitli, 256 bitli
134.	Xesh-funktsiyani natijasi …	uzunlikdagi xabar
135.	RSA algoritmi qanday jarayonlardan tashkil topgan	Kalitni generatsiyalash; Shifrlash; Deshifrlash.
136.	RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida necha bit bo'lishi talab etiladi.	2048
137.	Ma'lumotlar butunligi qanday algritmlar orqali amalga oshiriladi	Xesh funksiyalar
138.	To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub	Xalqa
139.	Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo'llamasligi mumkin	to'liq bog'lanishli
140.	Kompyuterning tashqi interfeysi deganda nima tushuniladi	kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidalari to'plamlari
141.	Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi	Yulduz
142.	Ethernet kontsentratori qanday vazifani bajaradi	kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi
143.	OSI modelida nechta sath mavjud	7
144.	OSI modelining to'rtinchi sathi qanday nomlanadi	Transport sathi
145.	OSI modelining beshinchi sathi qanday nomlanadi	Seanslar sathi
146.	OSI modelining birinchi sathi qanday nomlanadi	Fizik sath
147.	OSI modelining ikkinchi sathi qanday nomlanadi	Kanal sathi
148.	OSI modelining uchinchi sathi qanday nomlanadi	Tarmoq sathi
149.	OSI modelining oltinchi sathi qanday nomlanadi	Taqdimlash sathi
150.	OSI modelining ettinchi sathi qanday nomlanadi	Amaliy sath
151.	OSI modelining qaysi sathlari tarmoqqa bog'liq sathlar hisoblanadi	fizik, kanal va tarmoq sathlari
152.	OSI modelining tarmoq sathi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi	Marshrutizator
153.	Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi	Fizik sath
154.	Ma'lumotlarni uzatishning optimal marshrutlarini	Tarmoq sathi

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

176.	MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi	xavfsizlik siyosati ma’muri
177.	Agar sub’ektning xavfsizlik darajasida ob’ektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi	O‘qish
178.	Agar sub’ektning xavfsizlik darajasi ob’ektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.	Yozish
179.	Foydalanishni boshqarishning qaysi modelida har bir ob’ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun ob’ektlardan foydalanish ruxsati ko‘rsatiladi?	RBAC
180.	Rol tushunchasiga ta’rif bering.	Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin
181.	Foydalanishni boshqarishning qaysi usuli - ob’ektlar va sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.	ABAC
182.	XACML foydalanishni boshqarishni qaysi usulining standarti?	ABAC
183.	Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?	barchasi
184.	Axborotning kriptografik himoya vositalari necha turda?	3
185.	Dasturiy shifrlash vositalari necha turga bo‘linadi	4
186.	Diskni shifrlash nima uchun amalga oshiriladi?	Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
187.	Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?	4
188.	Kompyuter tarmoqlari bu –	Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi
189.	Tarmoq modeli –bu.. ikki	Hisoblash tizimlariorasidagi aloqani ularning ichki tuzilmaviy vatexnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir to‘plami
190.	OSI modelida nechta tarmoq sathi bor	7
191.	OSI modeli 7 stahi bu	Ilova
192.	OSI modeli 1 stahi bu	Fizik
193.	OSI modeli 2 stahi bu	Kanal
194.	TCP/IP modelida nechta satx mavjud	4
195.	Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi.	Shaxsiy tarmoq
196.	Tarmoq kartasi bu...	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim

		etadi.
197.	Switch bu...	Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
198.	Hab bu...	ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
199.	Tarmoq repiteri bu...	Signalni tiklash yoki qaytarish uchun foydalaniladi.
200.	Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi.	DNS tizimlari
201.	….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.	TCP
202.	…. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.	UDP
203.	Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi.	IP
204.	Tarmoq taxdidlari necha turga bo‘linadi	4
205.	Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;	Razvedka hujumlari
206.	Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi	Kirish hujumlari
207.	Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;	Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
208.	Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;	Zararli hujumlar
209.	Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?	Imzo qo‘yish va imzoni tekshirishdan
210.	Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi?	Imzo muallifining ochiq *kaliti yordamida*
211.	Tarmoq modeli-bu...	Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir
212.	OSI modeli nechta sathga ajraladi?	7
213.	Fizik sathning vazifasi nimadan iborat	Qurilma, signal va binar o‘zgartirishlar
214.	Ilova sathning vazifasi nimadan iborat	Ilovalarni tarmoqqa ulanish jarayoni
215.	Kanal sathning vazifasi nimadan iborat	Fizik manzillash
216.	Tarmoq sathning vazifasi nimadan iborat	Yo‘lni aniqlash va mantiqiy manzillash
217.	TCP/IP modeli nechta sathdan iborat	4
218.	Quyidagilarninf qaysi biri Kanal sathi protokollari	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35.
219.	Quyidagilarninf qaysi biri tarmoq sathi protokollari	. IP, ICMP, ARP, RARP
220.	Quyidagilarninf qaysi biri transport sathi protokollari	TCP, UDP, RTP

221.	Quyidagilarninf qaysi biri ilova sathi protokollari	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP va hak
222.	TCP/IP modelining kanal sathiga OSI modelining qaysi sathlari mos keladi	Kanal, Fizik
223.	TCP/IP modelining tarmoq sathiga OSI modelining qaysi sathlari mos keladi	Tarmoq
224.	TCP/IP modelining transport sathiga OSI modelining qaysi sathlari mos keladi	Tramsport
225.	TCP/IP modelining ilova sathiga OSI modelining qaysi sathlari mos keladi	Ilova, taqdimot, seans
226.	Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.	Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
227.	Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.	. Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
228.	Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang.	Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi
229.	Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang.	Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi
230.	Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan	Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi
231.	Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan	Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi
232.	Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan	Yuboriluvchi va qabul qilinuvchi ma’lumot TOKYeN yordamida manziliga yetkaziladi
233.	Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan	Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi
234.	Tarmoq kartasi nima?	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
235.	Repetir nima?	Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
236.	Hub nima?	Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
237.	Switch nima?	Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
238.	Router nima?	Qabul qilingan ma’lumotlarni tarmoq sathiga tegishli manzillarga ko‘ra (IP manzil) uzatadi
239.	DNS tizimlari.	Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi
240.	TCP bu- …	Transmission Control Protocol
241.	UDP bu-…	User datagram protocol

242.	Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang	Ichki, tashqi
243.	Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi	Biznes jarayonlarni to‘xtab qolishiga olib keladi
244.	Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi	Hujum natijasida ishlab chiqarishi yo‘qolgan hollarda uni qayta tiklash ko‘p vaqt talab qiladi va bu vaqtda ishlab chiqarish to‘xtab qoladi
245.	Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi	Konfidensial axborotni chiqib ketishi natijasida, tashkilot shaxsiy ma’lumotlarini yo‘qolishi mumkin
246.	Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi	Tashkilot xodimlarining shaxsiy va ishga oid ma’ulmotlarini kutilmaganda oshkor bo‘lishi ushbu xodimlarga bevosita ta’sir qiladi
247.	Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi	Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi
248.	Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi	tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi
249.	Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi.	Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.
250.	Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi	Razvedka hujumlari
251.	Ma’lumotlarni zaxira nusxalash bu – …	Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi
252.	Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz	Zaxira nusxalash
253.	Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering	Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
254.	Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi?	5
255.	Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi.	4
256.	Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash	Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart.
257.	RAID texnologiyasining transkripsiyasi qanday.	Random Array of Independent Disks
258.	RAID texnologiyasida nechta satx mavjud	6
259.	OSI modelining birinchi sathi qanday nomlanadi	Fizik sath
260.	OSI modelining ikkinchi sathi qanday nomlanadi	Kanal sathi
261.	OSI modelining uchinchi sathi qanday nomlanadi	Tarmoq sathi

262.	OSI modelining oltinchi sathi qanday nomlanadi	Taqdimlash sathi
263.	OSI modelining ettinchi sathi qanday nomlanadi	Amaliy sath
264.	Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi	Fizik sath
265.	Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub	TCP,UDP
266.	OSI modelining fizik sathi qanday funktsiyalarni bajaradi	Elektr signallarini uzatish va qabul qilish
267.	OSI modelining amaliy sathi qanday funktsiyalarni bajaradi	Klient dasturlari bilan o'zaro muloqotda bo'lish
268.	12 gacha bo'lgan va 12 bilan o'zaro tub bo'lgan sonlar soni nechta?	8 ta
269.	Yevklid algoritmi qanday natijani beradi?	Sonning eng katta umumiy bo'luvchisini toppish
270.	Qanday sonlar tub sonlar deb yuritiladi?	Faqatgina 1 ga va o'ziga bo'linadigan sonlar tub sonlar deyiladi.
271.	To‘liq zaxiralash	To‘liq va o‘sib boruvchi usullarning mujassamlashgan ko‘rinishi bo‘lib, oxirgi zaxiralangan nusxadan boshlab bo‘lgan o‘zgarishlarni zaxira nusxalab boradi. • Amalga oshirish to‘liq zaxiralashga qaraganda tez amalga oshiriladi. • Qayta tiklash o‘sib boruvchi zaxiralashga qaraganda tez amalga oshiriladi. • Ma’lumotni saqlash uchun to‘liq zaxiralashga qaraganda kam joy talab etadi
272.	O‘sib boruvchi zaxiralash	Zaxiralangan ma’lumotga nisbatan o‘zgarish yuz berganda zaxirilash amalga oshiriladi. • Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usuli bo‘lishi mumkin (to‘liq saxiralashdan). • Saqlash uchun kam hajm va amalga oshirish jarayoni tez
273.	Differensial zaxiralash	Ushbu zaxiralashda tarmoqga bog‘lanishamalga oshiriladi. • Iliq zaxiralashda, tizim yangilanishi davomiy yangilanishni qabul qilish uchun ulanadi
274.	Ushbu jarayon ma’lumot qanday yo‘qolgani, ma’lumotni qayta tiklash dasturiy vositasi va ma’lumotni tiklash manzilini qayergaligiga bog‘liq bo‘ladi. Qaysi jarayon	Ma’lumotlarni qayta tiklash
275.	Antivirus dasturlarini ko'rsating?	Drweb, Nod32, Kaspersky
276.	Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi	wep, wpa, wpa2
277.	Axborot himoyalangan qanday sifatlarga ega bo'lishi kerak?	ishonchli, qimmatli va to'liq
278.	Axborotning eng kichik o'lchov birligi nima?	bit
279.	Virtual xususiy tarmoq – bu?	VPN
280.	Xavfli viruslar bu - …	kompyuter ishlashida jiddiy nuqsonlarga sabab bo'luvchi viruslar
281.	Mantiqiy bomba – bu …	Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari

282.	Rezident virus...	tezkor xotirada saqlanadi
283.	DIR viruslari nimani zararlaydi?	FAT tarkibini zararlaydi
284.	.... kompyuter tarmoqlari bo'yicha tarqalib, komlg'yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o'zining nusxasini qoldiradi	«Chuvalchang» va replikatorli virus
285.	Mutant virus...	shifrlash va deshifrlash algoritmlaridan iborat-to'g'ri javob
286.	Fire Wall ning vazifasi...	tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta`minlaydi
287.	Kompyuter virusi nima?	maxsus yozilgan va zararli dastur
288.	Kompyuterning viruslar bilan zararlanish yo'llarini ko'rsating	disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali
289.	Troyan dasturlari bu...	virus dasturlar
290.	Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi?	5
291.	Antiviruslarni, qo'llanish usuliga ko'ra... turlari mavjud	detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar
292.	Axborotni himoyalash uchun ... usullari qo'llaniladi.	kodlashtirish, kriptografiya, stegonografiya
293.	Stenografiya mahnosi...	sirli yozuv
294.	…sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi	K.Shennon
295.	Kriptologiya yo'nalishlari nechta?	2
296.	Kriptografiyaning asosiy maqsadi...	maxfiylik, yaxlitlilikni ta`minlash
297.	Zararli dasturiy vositalarni aniqlash turlari nechta	3
298.	Signaiurana asoslangan	...bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin.
299.	O‘zgarishni aniqlashga asoslangan	Zararli dasturlar biror joyda joylashishi sababli, agar tizimdagi biror joyga o‘zgarishni aniqlansa, u holda u zararlanishni ko‘rsatishi mumkin
300.	Anomaliyaga asoslangan	Noodatiy yoki virusga o‘xshash yoki potensial zararli harakatlari yoki xususiyatlarni topishni maqsad qiladi
301.	Antiairuslar qanday usulda viruslarni aniqlaydi	Signaturaga asoslangan
302.	Viruslar -	o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi
303.	Rootkitlar-	ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma'lum harakatlarini yashiradi
304.	Backdoorlar -	zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish
305.	Troyan otlari-	bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan

		zararli koddan iborat bo‘ladi
306.	Ransomware-	mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi
307.	Resurslardan foydalanish usuliga ko’ra viruslar qanday turlarga bo’linadi	Virus parazit, Virus cherv
308.	Zararlagan obyektlar turiga ko’ra	Dasturiy, yuklanuvchi, Makroviruslar, multiplatformali viruslar
309.	Faollashish prinspiga ko’ra	Resident, Norezident
310.	Dastur kodini tashkil qilish yondashuviga ko‘ra	Shifrlangan, shifrlanmagan, Polimorf
311.	Shifrlanmagan viruslar	o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi.
312.	P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang	840
313.	256mod25=?	6
314.	bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi.	Tizim
315.	Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima duyidadi	Xavfsizlik siyosati
316.	RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday?	p va q –sonlarning ko‘paytmasini ifodalovchi sonning spektoriga teng;
317.	DES algoritmi akslantirishlari raundlari soni qancha?	16;
318.	DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha?	CHap qism blok 32 bit, o‘ng qism blok 32 bit;
319.	Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor?	SHifrlash va deshifrlash jarayonlari uchun kalitlarni generatsiya qilish qoidalariga ko‘ra farqlanadi
320.	19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta?	18 ta
321.	10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta?	4 ta
322.	Eyler funsiyasida $\phi(1)$ qiymati nimaga teng?	0
323.	Eyler funksiyasida 60 sonining qiymatini toping.	59
324.	Eyler funksiyasi yordamida 1811 sonining qiymatini toping.	1810
325.	97 tub sonmi?	Tub
326.	Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256.	244
327.	Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220	44
328.	Quyidagi ifodani qiymatini toping. -17mod11	5
329.	2 soniga 10 modul bo’yicha teskari sonni toping.	Ø
330.	Tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta’minlash sohasidagi tadbirlar tavsiflanadigan yuqori darajadagi reja nima?	Kiberxavfsizlik siyosati
331.	Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi?	tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi

332.	Kiberxavfsizlikni ta’minlash masalalari bo’yicha xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang	SANS (System Administration Networking and Security)
333.	Korxonaning davomli muvaffaqiyat bilan faoliyat yuritishini ta’minlashga mo’ljallangan strukturalangan va o’zaro bog’langan harakatlar to’plami- …	Strategiya
334.	Tahdidlarning muvaffaqiyatli amalga oshirilishiga imkon beruvchi har qanday omil – bu …	Zaiflik
335.	ISO/IEC 27002:2005 – ….	Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari
336.	O’zDStISO/IEC 27005:2013 – ….	Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish
337.	Axborot xavfsizligi arxitekturasining nechta satxi bor?	3
338.	Rahbariy hujjat. Ma’lumotlar uzatish tarmog’ida axborot xavfsizligini ta’minlash to’g’risida Nizom - Xujjat raqamini toping	RH 45-215:2009
339.	Davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta’minlash dasturini ishlab chiqish tartibi - Xujjat raqamini toping	RH 45-185:2011
340.	Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta’minlash darajasini aniqlash tartibi - Xujjat raqamini toping	RH 45-193:2007
341.	Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta’riflar - Xujjat raqamini toping	TSt 45-010:2010
342.	Quyidagilardan qaysi standart aloqa va axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta’riflarni belgilaydi?	TSt 45-010:2010
343.	Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni nima?	Identifikatsiya
344.	Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima?	Autentifikatsiya
345.	Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni – nima deyiladi?	Avtorizatsiya
346.	Identifikatsiya nima?	Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni
347.	Autentifikatsiya nima?	Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni
348.	Avtorizatsiya nima?	Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni
349.	... - Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o’tishni ta’minlovchi	Parol

	biror axborot	
350.	Smart karta o'lchamidagi, kichik xajmdagi xotira va xisoblash imkoniyatiga ega bo'lgan, o'zida parol yoki kalitni saqlovchi qurilma nima deb ataladi?	Token, Smartkarta
351.	Smarkarta nima asosida autentifikatsiyalaydi?	Something you have
352.	Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o'zgarib turadigan parol nima deyiladi?	One-time password (OTP)
353.	Foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish nima deb ataladi?	Ma'murlash
354.	Amaldagi qonunchilikka mos ravishda texnik, dasturiy va dasturiy-texnik vositalar yordamida axborot xavfsizligining nokriptografik usullari bilan ta'minlashni inobatga oluvchi axborot himoyasi nima?	Axborotning texnik himoyasi
355.	Nazorat hududi – bu ...	Qo'riqlanuvchi soha bo'lib, uning ichida kommunikatsiya qurilmalari hamda axborot tarmog'ining lokal tarkibiy qurilmalarini birlashtiruvchi barcha nuqtalar joylashadi
356.	Texnik himoya vositalari – bu ...	Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob'ektni himoyalashdir
357.	Bu axborotni tutib olish qurilmasi bo'lib, ularda uzatuvchi qurilma sifatida kontaktli mikrofonlardan foydalaniladi	Stetoskoplar
358.	Xesh funktsiya to'g'ri ko'rsatilgan javobni aniqlang.	MD5
359.	MD5, SHA1, Tiger xesh funktsiyalari uchun blok uzunligi necha baytga teng?	64 bayt
360.	Sub'ektni ob'ektga ishlash qobilyatini aniqlash – nima?	Foydalanishni boshqarish
361.	Foydalanishni boshqarishda sub'ekt bu -	Inson, dastur, jarayon
362.	Foydalanishni boshqarishning qaysi usuli tizimdagi shaxsiy ob'ektlarni ximoyalash uchun qo'llaniladi?	Discretionary access control DAC
363.	Foydalanishni boshqarishning qaysi usulidan asosan operatsion tizimlarda qo'llaniladi?	Discretionary access control DAC
364.	Foydalanishni boshqarishning qaysi usulida foydalanishlar sub'ektlar va ob'ektlarni klassifikatsiyalashga asosan boshqariladi?	Mandatory access control MAC
365.	Foydalanishni boshqarishning qaysi usulida xavfsizlik markazlashgan tarzda xavfsizlik siyosati m'muri tomonidan amalga oshiriladi?	Mandatory access control MAC
366.	Foydalanishni boshqarishning qaysi usulida xar bir foydalanuvchini foydalanish ruxsatini belgilash o'rniga rol uchun ob'ektlardan foydalanish ruxsatini ko'rsatish yetarli bo'ladi?	Role-based access control RBAC
367.	Foydalanishni boshqarishning qaysi usulida sub'ekt va ob'ektlarga tegishli xuquqlarni ma'murlash oson kechadi?	Role-based access control RBAC
368.	Firibgarlikni oldini olish uchun bir shaxs tomonidan ko'plab vazifalarni bajarishga ruxsat bermaslik zarur. Bu muammo foydalanishni boshqarishni qaysi usulida bartaraf etiladi?	Role-based access control RBAC

369.	Ob’ekt va sub’ektlarning attributlari, ular bilan mumkin bo’lgan amallar va so’rovlarga mos keladigan muxit uchun qoidalarni taxlil qilish asosida foydalanishni boshqarish -	Attribute based access control ABAC
370.	Attribute based access control ABAC usuli attributlari qaysilar?	Foydalanuvchi attributlari, Resurs attributlari, Ob’ekt va muxit attributlari
371.	Foydalanishni boshqarishning qaysi usulida ruxsatlar va xarakatni kim bajarayotganligi to’g’risidagi xolatlar “agar, u xolda” buyrug’idan tashkil topgan qoidalarga asoslanadi?	Attribute based access control ABAC
372.	XASML standarti foydalanishni boshqarishning qaysi usulida qo’llaniladi?	Attribute based access control ABAC
373.	XASML standartida qoida nima?	Maqsad, ta’sir, shart, majburiyat va maslaxatlar
374.	XASML standartida maqsad nima?	Sub’ekt ob’ekt ustida nima xarakat qilishi
375.	Lampsonning foydalanishni boshqarish matritsasi nimalardan tashkil topgan?	Imtiyozlar ro’yxati
376.	Access control list va Capability list bu nimaning asosiy elementi xisoblanadi?	Lampson matritsasining
377.	Lampson matritsasining satrlarida nima ifodalanadi?	Sub’ektlar
378.	Foydalanishni boshqarishning mantiqiy vositalari infratuzilma va uning ichidagi tizimlarda ... uchun foydalaniladi.	Mandat, Tasdiqlash, Avtorizatsiya
379.	SHaxsiy simsiz tarmoq standartini aniqlang.	Bluetooth, IEEE 802.15, IRDA
380.	Lokal simsiz tarmoq standartini aniqlang.	IEEE 802.11, Wi-Fi, HiperLAN
381.	Regional simsiz tarmoq standartini aniqlang.	IEEE 802.16, WiMAX
382.	Global simsiz tarmoq standartini aniqlang.	CDPD, 2G, 2.5G, 3G, 4G, 5G
383.	Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang.	SHaxsiy simsiz tarmoq
384.	IEEE 802.11, Wi-Fi, HiperLAN standartida ishlovchi simsiz tarmoq turini aniqlang.	Lokal simsiz tarmoq
385.	IEEE 802.16, WiMAX standartida ishlovchi simsiz tarmoq turini aniqlang.	Regional simsiz tarmoq
386.	CDPD, 2G, 2.5G, 3G, 4G, 5G standartida ishlovchi simsiz tarmoq turini aniqlang.	Global simsiz tarmoq
387.	Bluetooth qanday chastota oralig’ida ishlaydi?	2.4-2.485 Ggts
388.	Wi-Fi qanday chastota oralig’ida ishlaydi?	2.4-5 Ggts
389.	WiMax tarmog’ining tezligi qancha?	1 Gbit/sekund
390.	Quyidagilardan qaysi biri MITM xujumiga tegishli xatti-xarakat ximoblanadi?	Aloqa seansini konfidentsialligini va yaxlitligini buzish
391.	WiMAX tarmoq arxitekturasi nechta tashkil etuvchidan iborat?	5
392.	WiMAX tarmoq arxitekturasi qaysi tashkil etuvchidan iborat?	Base station, Subscriber station, Mobile station, Relay station, Operator network
393.	GSM raqamli mobil telefonlarining nechanchi avlodi uchun ishlab chiqilgan protokol?	Ikkinchi avlodi
394.	GSM standarti qaysi tashkilot tomonidan ishlab chiqilgan?	European telecommunications standards institute
395.	.... – o’zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma’lumoti va xavfsizlik	Sim karta

	algoritmlarini saqlaydi.	
396.	Rutoken S qurilmasining og’irligi qancha?	6.3 gramm
397.	True Crypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?	AES, Serpent, Twofish
398.	Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidentsialligini aniqlash qaysi dasturiy shifrlash vositalarining vazifasi?	Disc encryption software
399.	BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?	AES, Serpent, Twofish
400.	AxCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?	AES-256
401.	Qog’oz ko’rinishidagi axborotlarni yo’q qilish qurilmasining nomini kiriting.	Shreder
402.	Ma’lumotlarni bloklarga bo’lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?	RAID 0
403.	Qaysi texnologiyada ma’lumotni ko’plab nusxalari bir vaqtda bir necha disklarga yoziladi?	RAID 1
404.	Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi?	RAID 3
405.	Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?	RAID 5
406.	Disk zararlanganda “qaynoq almashtirish” yordamida uni almashtirish mumkin. Bu xususiyat qaysi texnologiyaga tegishli?	RAID 50
407.	Zaxiralashning qanday turlari mavjud?	To’liq, o’sib boruvchi, differentsial
408.	IOS, Android, USB xotiralardan ma’lumotlarni tiklash uchun qaysi dasturdan foydalaniladi?	EASEUS Data recovery wizard
409.	Foydalanuvchi ma’lumotlarini qo’lga kirituvchi va uni xujumchiga yuboruvchi dasturiy kod nima?	Spyware
410.	Operatsion tizim tomonidan aniqlanmasligi uchun ma’lum xarakatlarni yashirish nima deyiladi?	Rootkits
411.	Qurbon kompyuterda mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo’yib to’lov amalga oshirishni talab qiladi. Bu qaysi zararli dastur?	Ransomware
412.	Quyidagilardan o’zidan ko’payishi yo’q bo’lganlarini belgilang.	Mantiqiy bomba, Troyan oti, Backdoors
413.	Viruslar resurslardan foydalanish usuliga ko’ra qanday turlarga bo’linadi?	Virus parazitlar, virus chervlar
414.	Viruslar zararlangan ob’ektlar turiga ko’ra qanday turlarga bo’linadi?	Dasturiy, yuklanuvchi, makroviruslar, ko’p platformali
415.	Viruslar faollashish printsipiga ko’ra qanday turlarga bo’linadi?	Rezident, norezident
416.	Viruslar dastur kodini tashkil qilish yondoshuviga ko’ra qanday turlarga bo’linadi?	SHifrlangan, shifrlanmagan, polimorf
417.	Dastlabki virus nechanchi yilda yaratilgan?	1988
418.	ILOVEYOU virusi keltirgan zarar qancha?	10 mlrd. Dollar
419.	CodeRed virusi keltirgan zarar qancha?	2 mlrd. Dollar
420.	Melissa virusi keltirgan zarar qancha?	80 million dollar
421.	NetSky virusi keltirgan zarar qancha?	18 mlrd. Dollar

422.	MyDoom virusi keltirgan zarar qancha?	38 mlrd. Dollar
423.	Risk monitoring ….. ni paydo bo'lish imkoniyatini aniqlaydi.	Yangi risklar
424.	….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.	Risk monitoring
425.	Axborot xavfsizligi siyoatining necha hil turi bor?	3
426.	Internetdan foydalanish siyosatining nechta turi mavjud?	4
427.	Nomuntazam siyosat (Promiscuous Policy) nima?	Tizim resurslaridan foydalanishda hech qanday cheklovlar qo'ymaydi
428.	Paranoid siyosati (Paranoid Policy) – bu ….	Hamma narsa ta'qiqlanadi
429.	Ruxsat berishga asoslangan siyosat (Permissive Policy) – bu …	Faqat ma'lum hizmatlar/hujumlar/harakatlar bloklanadi
430.	Ehtiyotkorlik siyosati (Prudent Policy) – bu ….	Barcha hizmatlar blokirovka qilingandan so'ng bog'lanadi
431.	Tizim resurslaridan foydalanishda hech qanday cheklovlar qo'ymaydi. Bu qaysi xavfsizlik siyosatiga hos?	Nomuntazam siyosat (Promiscuous Policy)
432.	Barcha hizmatlar blokirovka qilingandan so'ng bog'lanadi. Bu qaysi xavfsizlik siyosatiga hos?	Ehtiyotkorlik siyosati (Prudent Policy)
433.	Faqat ma'lum hizmatlar/hujumlar/harakatlar bloklanadi. Bu qaysi xavfsizlik siyosatiga hos?	Ruxsat berishga asoslangan siyosat (Permissive Policy)
434.	Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?	Paranoid siyosati (Paranoid Policy)
435.	Tizim arxitekturasining turlari nechta?	5
436.	Internet, havo hujumidan mudofaa, transport tizimlari qaysi tizim arxitekturasiga xos?	Hamkorlik tizimlari arxitekturasi
437.	Cloud computing texnologiyasining nechta asosiy turi mavjud?	3
438.	Raqamli soatlar qaysi texnologiyaga tegishli?	O'rnatilgan tizimlar (Embedde systems)
439.	Xavfsizlikning asosiy yo'nalishlarini sanab o'ting.	*Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik
440.	Axborot xavfsizligining asosiy maqsadlaridan biri-bu…	*Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish
441.	Konfidentsiallikga to'g'ri ta`rif keltiring.	*axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
442.	Yaxlitlikni buzilishi bu - …	*Soxtalashtirish va o'zgartirish
443.	... axborotni himoyalash tizimi deyiladi.	*Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo'qotilishiga to'sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi
444.	Kompyuter virusi nima?	*maxsus yozilgan va zararli dastur
445.	Axborotni himoyalash uchun ... usullari qo'llaniladi.	*kodlashtirish, kriptografiya, stegonografiya
446.	Stenografiya ma'nosi...	*sirli yozuv
447.	Kriptografiyaning asosiy maqsadi...	*maxfiylik, yaxlitlilikni ta`minlash
448.	SMTP - Simple Mail Transfer protokol nima?	*elektron pochta protokoli
449.	SKIP protokoli...	*Internet protokollari uchun kriptokalitlarning

		oddiy boshqaruvi
450.	Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar…	*uzilish, tutib qolish, o’zgartirish, soxtalashtirish
451.	...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.	*konfidentsiallik
452.	Foydalanish huquqini cheklovchi matritsa modeli bu...	*Bella La-Padulla modeli
453.	Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi?	*TCP/IP, X.25 protokollar
454.	Himoya tizimi kompleksligiga nimalar orqali erishiladi?	*Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali
455.	Kalit – bu …	*Matnni shifrlash va shifrini ochish uchun kerakli axborot
456.	Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?	*simmetrik kriptotizimlar
457.	Autentifikatsiya nima?	*Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi
458.	Identifikatsiya bu- …	*Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni
459.	O’rin almashtirish shifri bu - …	*Murakkab bo’lmagan kriptografik akslantirish
460.	Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.	*2 turga
461.	Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular …	*hosil qilish, yig’ish, taqsimlash
462.	Kriptologiya -	*axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
463.	Kriptografiyada alifbo –	*axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
464.	Simmetrik kriptotizimlarda ... jumlani davom ettiring	*shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi
465.	Kriptobardoshlilik deb …	*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
466.	Elektron raqamli imzo deb –	*xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
467.	Kriptografiya –	*axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
468.	Kriptografiyada matn –	*alifbo elementlarining tartiblangan to’plami
469.	Kriptoanaliz –	*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
470.	Shifrlash –	*akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi
471.	Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi?	*Tez, aniq va maxfiyligiga
472.	Faol hujum turi deb…	*Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon
473.	Blokli shifrlash-	*shifrlanadigan matn blokiga qo’llaniladigan

		asosiy akslantirish
474.	Simmetrik kriptotizmning uzluksiz tizimida …	*ochiq matnning har bir harfi va simvoli alohida shifrlanadi
475.	Kripto tizimga qo’yiladigan umumiy talablardan biri	*shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak
476.	Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?	*Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi
477.	Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang	*Vijener matritsasi, Sezar usuli
478.	Akslantirish tushunchasi deb nimaga aytiladi?	*1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga
479.	Simmetrik guruh deb nimaga aytiladi?	*O’rin almashtirish va joylashtirish
480.	Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?	*simmetrik kriptosistemalar
481.	Xavfli viruslar bu - …	*kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar
482.	Mantiqiy bomba – bu …	*Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari
483.	Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?	*raqamli imzoni shakllantirish va tekshirish muolajasi
484.	Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi?	*Simmetrik va assimetrik
485.	Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?	*Korporativ va umumfoydalanuvchi
486.	Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo’linadi?	*Sust va faol
487.	Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?	*SMTP, POP yoki IMAR
488.	Axborot resursi – bu?	*axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi
489.	Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu?	*login
490.	Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu?	*parol
491.	Identifikatsiya jarayoni qanday jarayon?	* axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
492.	Autentifikatsiya jarayoni qanday jarayon?	*obyekt yoki subhektni unga berilgan

		identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
493.	Avtorizatsiya jarayoni qanday jarayon?	*foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
494.	Ro'yxatdan o'tish bu?	*foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
495.	Axborot qanday sifatlarga ega bo'lishi kerak?	*ishonchli, qimmatli va to'liq
496.	Axborotning eng kichik o'lchov birligi nima?	*bit
497.	Elektron hujjatning rekvizitlari nechta qismdan iborat?	*4
498.	Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?	*fleshka, CD va DVD disklar
499.	Imzo bu nima ?	*hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati.
500.	Muhr bu nima?	*hujjatning haqiqiyligini va biror bir yuridik shaxsga tegishli ekanligini tasdiqlovchi isbotdir
501.	DSA – nima	*Raqamli imzo algoritmi
502.	El Gamal algoritmi qanday algoritm	*Shifrlash algoritmi va raqamli imzo algoritmi
503.	Sezarning shifrlash sistemasining kamchiligi	*Harflarning so'zlarda kelish chastotasini yashirmaydi
504.	Axborot xavfsizligi va xavfsizlik san'ati haqidagi fan …. deyiladi?	*Kriptografiya
505.	Tekstni boshqa tekst ichida ma'nosini yashirib keltirish bu -	*steganografiya
506.	Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?	*Deshifrlash
507.	…… – hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.	*Kiberxavfsizlik
508.	Risk	*Potensial foyda yoki zarar
509.	Tahdid nima?	*Tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.
510.	Kodlash nima?	*Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir
511.	Shifrlash nima?	Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir
512.	Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug'ullanadi	Kriptoanaliz
513.	Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi	$\{d, e\}$ – ochiq, $\{e, n\}$ – yopiq;
514.	Zamonaviy kriptografiya qanday bo'limlardan iborat?	Electron raqamli imzo; kalitlarni boshqarish

515.	Kriptografik usullardan foydalanishning asosiy yo'nalishlari nimalardan iborat?	uzatiliyotgan xabarlarni haqiqiyligini aniqlash
516.	Shifr nima?	* Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan krptografik algoritm
517.	Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?	*Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi
518.	Oqimli shifrlashning mohiyati nimada?	Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma'lumotlarnbi bitlar yoki belgilar bo'yicha shifrlaydi
519.	Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating.	*uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmasligi uchun algoritm yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog'liq bo'lishi lozim,
520.	Kriptotizim qaysi komponentlardan iborat?	*ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, Ek : M $\rightarrow$ C (shifrlash uchun) va Dk: C$\rightarrow$M (deshifrlash uchun) funktsiyalar
521.	Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?	*shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun
522.	Kriptografik elektron raqamli imzolarda qaysi kalitlar ma'lumotni yaxlitligini ta'minlashda ishlatiladi.	*ochiq kalitlar
523.	Xesh-funktsiyani natijasi …	Kiruvchi xabar uzunligidan uzun xabar
524.	RSA algoritmi qanday jarayonlardan tashkil topgan	*Kalitni generatsiyalash; Shifrlash; Deshifrlash.
525.	Ma'lumotlar butunligi qanday algritmlar orqali amalga oshiriladi	*Xesh funksiyalar
526.	To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub	*Xalqa
527.	Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo'llamasligi mumkin?	*to'liq bog'lanishli
528.	Kompyuterning tashqi interfeysi deganda nima tushuniladi?	*kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidalari to'plamlari
529.	Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?	*Yulduz
530.	Ethernet kontsentratori qanday vazifani bajaradi	*kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi
531.	OSI modelida nechta satx mavjud	*7
532.	OSI modelining to'rtinchi satxi qanday nomlanadi	*Transport satxi

533.	OSI modelining beshinchi satxi qanday nomlanadi	*Seanslar satxi
534.	OSI modelining birinchi satxi qanday nomlanadi	*Fizik satx
535.	OSI modelining ikkinchi satxi qanday nomlanadi	*Kanal satxi
536.	OSI modelining uchinchi satxi qanday nomlanadi	*Tarmoq satxi
537.	OSI modelining oltinchi satxi qanday nomlanadi	*Taqdimlash satxi
538.	OSI modelining yettinchi satxi qanday nomlanadi	*Amaliy satx
539.	OSI modelining qaysi satxlari tarmoqqa bog'liq satxlar hisoblanadi	*fizik, kanal va tarmoq satxlari
540.	OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi	*Marshrutizator
541.	Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi	*Fizik satx
542.	Ma'lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi	*Tarmoq satxi
543.	Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub	*IP, IPX
544.	Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub	*TCP,UDP
545.	OSI modelining fizik satxi qanday funktsiyalarni bajaradi	*Elektr signallarini uzatish va qabul qilish
546.	OSI modelining amaliy satxi qanday funktsiyalarni bajaradi	*Klient dasturlari bilan o'zaro muloqotda bo'lish
547.	Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub	*Ethernet, FDDI
548.	Keltirilgan protokollarning qaysilari taqdimlash satxi protokollariga mansub	*SNMP, Telnet
549.	Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan amallarga ruxsat berish jarayoni bu...	*Avtorizatsiya
550.	Autentifikatsiya faktorlari nechta	4
551.	Faqat foydalanuvchiga ma'lum va biror tizimda autentifikatsiya jarayonidan o'tishni ta'minlovchi biror axborot nima	Login
552.	Ko'z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar?	Biron nimaga egalik asosida
553.	barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi?	*Fizik satx
554.	Fizik xavfsizlikda Yong'inga qarshi tizimlar necha turga bo'linadi	*2
555.	Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?	*Foydalanishni boshqarish
556.	Foydalanishni boshqarish –bu...	Subyektni Subyektga ishlash qobilyatini aniqlashdir.
557.	Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?	Obyekt
558.	Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ?	*Obyekt

559.	Foydalanishna boshqarishning nechta usuli mavjud?	*4
560.	Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo‘llaniladi	ABAC
561.	Foydalanishni boshqarishning qaysi modelida Obyekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi	ABAC
562.	Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi.	ABAC
563.	Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bog‘liq..	Tashkilotda Obyektning muhimlik darajasi bilan yoki yuzaga keladigan foyda miqdori bilan bilan xarakterlanadi
564.	MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi	*xavfsizlik siyosati ma’muri
565.	Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi	Yozish
566.	Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.	*Yozish
567.	Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun Obyektlardan foydalanish ruxsati ko‘rsatiladi?	ABAC
568.	Rol tushunchasiga ta’rif bering.	*Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin
569.	Foydalanishni boshqarishning qaysi usuli - Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.	*ABAC
570.	XACML foydalanishni boshqarishni qaysi usulining standarti?	*ABAC
571.	Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?	*barchasi
572.	Axborotning kriptografik himoya vositalari necha turda?	4
573.	Dasturiy shifrlash vositalari necha turga bo‘linadi	*4
574.	Diskni shifrlash nima uchun amalga oshiriladi?	*Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
575.	Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?	8
576.	Kompyuter tarmoqlari bu –	*Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi
577.	Tarmoq modeli –bu.. ikki	Matematik modellar to‘plami

578.	OSI modelida nechta tarmoq satxi bor	*7
579.	OSI modeli 7 satxi bu	*Ilova
580.	OSI modeli 1 satxi bu	Ilova
581.	OSI modeli 2 satxi bu	Ilova
582.	TCP/IP modelida nechta satx mavjud	*4
583.	Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi?	Lokal
584.	Tarmoq kartasi bu...	*Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
585.	Switch bu...	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
586.	Hab bu...	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
587.	Tarmoq repiteri bu...	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
588.	Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi.	*DNS tizimlari
589.	….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.	*TCP
590.	…. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.	*UDP
591.	Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi.	TCP
592.	Tarmoq taxdidlari necha turga bo‘linadi	2
593.	Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;	*Razvedka hujumlari
594.	Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi	Razvedka hujumlari
595.	Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;	Razvedka hujumlari
596.	Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;	Razvedka hujumlari
597.	RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart?	*e soni Eyler funksiyasi - $\varphi(n)$ bilan o‘zaro tub
598.	RSA elektron raqamli imzo algoritmidagi yopiq kalit d qanday hisoblanadi? Bu yerda p va q tub sonlar,n=pq, $\varphi(n)$- Eyler funksiyasi,e-ochiq kalit	* $d = e^{-1} mod \varphi(n)$

599.	Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?	*Imzo qo‘yish va imzoni tekshirishdan
600.	Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi?	*Imzo muallifining ochiq *kaliti yordamida*
601.	**Tarmoq modeli-bu...**	*Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir
602.	OSI modeli nechta satxga ajraladi?	2
603.	Fizik satxning vazifasi nimadan iborat	*Qurilma, signal va binar o‘zgartirishlar
604.	Ilova satxning vazifasi nimadan iborat	Qurilma, signal va binar o‘zgartirishlar
605.	Kanal satxning vazifasi nimadan iborat	Qurilma, signal va binar o‘zgartirishlar
606.	Tarmoq satxning vazifasi nimadan iborat	Qurilma, signal va binar o‘zgartirishlar
607.	TCP/IP modeli nechta satxdan iborat	*4
608.	Quyidagilarninf qaysi biri Kanal satxi protokollari	*Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35.
609.	Quyidagilarninf qaysi biri tarmoq satxi protokollari	Ethernet, Token Ring,FDDI, X.25, Frame Relay, RS-232, v.35.
610.	Quyidagilarninf qaysi biri transport satxi protokollari	Ethernet, Token Ring,FDDI, X.25, Frame Relay, RS-232, v.35.
611.	Quyidagilarninf qaysi biri ilova satxi protokollari	Ethernet, Token Ring,FDDI, X.25, Frame Relay, RS-232, v.35.
612.	TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi	*Kanal, Fizik
613.	TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi	Kanal, Fizik
614.	TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi	Kanal, Fizik
615.	TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos keladi	Kanal, Fizik
616.	Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.	*Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
617.	Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.	Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
618.	Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang.	Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
619.	Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang.	Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
620.	Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan	*Tarmoqda har bir kompyuter yoki tugun Markaziy tugunga individual bog‘langan bo‘ladi
621.	Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan	Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi
622.	Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan	Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi

623.	Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan	Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi
624.	Tarmoq kartasi nima?	*Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
625.	Repetir nima?	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
626.	Hub nima?	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
627.	Switch nima?	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
628.	Router nima?	Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
629.	DNS tizimlari.	*Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi
630.	TCP bu- …	*Transmission Control Protocol
631.	UDP bu-…	User domain protocol
632.	IP protokolining necha xil versiyasi mavjud?	1
633.	Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang	*Ichki, tashqi
634.	Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi	*Biznes jarayonlarni to‘xtab qolishiga olib keladi
635.	Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi	Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi
636.	Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi	Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi
637.	Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi	Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi
638.	Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi	*Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi
639.	Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi	Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi
640.	Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi.	Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi
641.	Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi	*Razvedka hujumlari
642.	Razvedka hujumiga berilgan ta’rifni aniqlang	*Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni

		to‘plashni maqsad qiladi;
643.	Kirish hujumiga berilgan ta’rifni aniqlang	asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axboro ni to‘plashni maqsad qiladi;
644.	DOS hujumiga berilgan ta’rifni aniqlang	asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;
645.	Zararli hujumga berilgan ta’rifni aniqlang	asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;
646.	Razvetka hujumari necha turga bo’linadi	1
647.	Qaysi hujum jarayoni TCP/IP tarmog‘ida paketlarni tutib olish, dekodlash, tekshirish va tarjima qilishni o‘z ichiga oladi	*Paketlarni snifferlash
648.	Tarmoqlaro ekranni OSI modeli bo’yicha qanday turlarga bo’lindi?	*• paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida
649.	Tarmoqlaro ekranni foydalanilgan texnologiyasi bo’yicha qanday turlarga bo’lindi?	paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida
650.	Tarmoqlaro ekranni bajarilishiga ko’ra qanday turlarga bo’lindi?	paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida
651.	Tarmoqlaro ekranni ulanish sxemasi bo’yicha qanday turlarga bo’lindi?	paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahidaishlaydi; ilova proksilari – ilova satxida
652.	Paket filtrlari tarmoqlararo ekrani vazifasi nima?	*Tarmoq satxida paketlarni tahlillashga asoslan;
653.	Ilova proksilari tarmoqlararo ekrani vazifasi nima?	Tarmoq satxida paketlarni tahlillashga asoslan;
654.	Ekspert paket filtrlari tarmoqlararo ekrani vazifasi nima?	Tarmoq satxida paketlarni tahlillashga asoslan;
655.	Quyidagilardan qaysi biri paket filtrlari tarmoqlararo ekrani kamchiligini ifodalaydi.	*Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma’lumotlarni, zararli dasturlarni va hak. tekshirmaydi.
656.	Quyidagilardan qaysi biri ekspert paket filtrlari tarmoqlararo ekrani kamchiligini ifodalaydi.	Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma’lumotlarni, zararli dasturlarni va hak. tekshirmaydi.
657.	Simsiz tarmoqlarning nechta turi mavjud	5
658.	Bluetooth qanday simsiz tarmoq turiga kiradi.	Global
659.	Wifi qanday simsiz tarmoq turiga kiradi.	Global
660.	LTE, CDMA, HSDPA qanday simsiz tarmoq turiga kiradi.	*Global
661.	WiMAX qanday simsiz tarmoq turiga kiradi.	Global
662.	Bluetooth texnologiyasida autentifikatsiya bu…	Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish.
663.	Bluetooth texnologiyasida konfidensiallik bu…	*Ikki autentifikatsiyalangan tarmoqda

		ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish.
664.	Bluetooth texnologiyasida avtorizatsiya bu…	Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish.
665.	GSM bu ..-	*Global System for Mobile Communications
666.	Simsiz tarmoq Bluetooth ishlash rejimlari nechta?	2
667.	Kompyuterda hodisalar haqidagi ma’lumot qayerda saqlanadi?	*hodisalar jurnaliga
668.	Windows operatsion tizimida xatolik hodisasiga berilgan ta’rifni belgilang.	*Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi.
669.	Windows operatsion tizimida ogohlantirish hodisasiga berilgan ta’rifni belgilang.	Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi.
670.	Windows operatsion tizimida axborot hodisasiga berilgan ta’rifni belgilang.	Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi.
671.	Windows operatsion tizimida muvaffaqiyatli audit hodisasiga berilgan ta’rifni belgilang.	Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi.
672.	Windows operatsion tizimida muvaffaqiyatsiz audit hodisasiga berilgan ta’rifni belgilang.	Ma’lumotni yo‘qotish yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd yetiladi.
673.	Ma’lumotlarni zaxira nusxalash bu – …	*Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi
674.	Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz	*Zaxira nusxalash
675.	Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering	*Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
676.	Ma’lumotlarni g’arazli hatti harakatlar yo’qolish sababiga ta’rif bering	Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini

		to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
677.	Ma’lumotlarni tasodifiy sabablar tufayli yo’qolish sababiga ta’rif bering	Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
678.	Ma’lumotlarni tabiiy ofatlar tufayli yo’qolish sababiga ta’rif bering	Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
679.	Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi?	7
680.	Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi.	*4
681.	Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash	*Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart.
682.	Zaxira nusxalovchi vositalar tanlashdagi *ishonchlilik* xuusiyatiga berilgan ta’rifni nelgilash	Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart.
683.	Zaxira nusxalovchi vositalar tanlashdagi tezlik xuusiyatiga berilgan ta’rifni nelgilash	Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart.
684.	Zaxira nusxalovchi vositalar tanlashdagi foydalanuvchanlik xuusiyatiga berilgan ta’rifni nelgilash	Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart.
685.	Zaxira nusxalovchi vositalar tanlashdagi qulaylik xuusiyatiga berilgan ta’rifni nelgilash	Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart.
686.	RAID texnologiyasining transkripsiyasi qanday.	Redundant Array of Independent Disks
687.	RAID texnologiyasida nechta satx mavjud	3
688.	RAID 0: diskni navbatlanishi bu-..	*Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi. Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi
689.	RAID 1: diskni navbatlanishi bu-..	Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi. Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi
690.	RAID 3: diskni navbatlanishi bu-..	Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga bo‘lish orqali yaxshilaydi. Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi
691.	RAID 5: diskni navbatlanishi bu-..	Ma’lumotni bloklarga bo‘lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko‘plab kanal va disk drayverlariga

		bo‘lish orqali yaxshilaydi. Agar disk buzilsa, ma’lumotni tiklab bo‘lmaydi. • Kamida ikkita disk talab qilinadi
692.	RAID 10: diskni navbatlanishi bu-..	*Gibrid satx bo‘lib, RAID 1 va RAID 0 satxlaridan iborat va kamida 4 ta diskni talab etadi
693.	RAID 50: diskni navbatlanishi bu-..	Gibrid satx bo‘lib, RAID 1 va RAID 0 satxlaridan iborat va kamida 4 ta diskni talab etadi
694.	Ma’lumotlarni nusxalash usullari necha xil usulda amalga oshiriladi?	*3
695.	Issiq zaxiralash usuliga berilgan ta’rifni belgilang.	*Ushbu usulda foydalanuvchi tizimni boshqarayotgan vaqtda ham zaxira nusxalash jarayoni davom ettiriladi. Mazkur zaxiralash usulini amalga oshirish tizimni harakatsiz vaqtini kamaytiradi.
696.	Iliq zaxiralash usuliga berilgan ta’rifni belgilang.	Ushbu usulda foydalanuvchi tizimni boshqarayotgan vaqtda ham zaxira nusxalash jarayoni davom ettiriladi. Mazkur zaxiralash usulini amalga oshirish tizimni harakatsiz vaqtini kamaytiradi.
697.	Sovuq zaxiralash usuliga berilgan ta’rifni belgilang.	Ushbu usulda foydalanuvchi tizimni boshqarayotgan vaqtda ham zaxira nusxalash jarayoni davom ettiriladi. Mazkur zaxiralash usulini amalga oshirish tizimni harakatsiz vaqtini kamaytiradi.
698.	Ichki zahiralash qanday amalga oshiriladi	Ichki zahiralashda mahalliy yoki global serverlardan foydalaniladi
699.	OSI modelining birinchi satxi qanday nomlanadi	*Fizik satx
700.	OSI modelining ikkinchi satxi qanday nomlanadi	*Kanal satxi
701.	OSI modelining uchinchi satxi qanday nomlanadi	*Tarmoq satxi
702.	OSI modelining oltinchi satxi qanday nomlanadi	*Taqdimlash satxi
703.	OSI modelining ettinchi satxi qanday nomlanadi	*Amaliy satx
704.	Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi	*Fizik satx
705.	Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub	*TCP,UDP
706.	OSI modelining fizik satxi qanday funktsiyalarni bajaradi	*Elektr signallarini uzatish va qabul qilish
707.	OSI modeliningamaliy satxi qanday funktsiyalarni bajaradi	*Klient dasturlari bilan o’zaro muloqotda bo’lish
708.	12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan sonlar soni nechta?	6 ta
709.	Yevklid algoritmi qanday natijani beradi?	*Sonning eng katta umumiy bo’luvchisini toppish
710.	Qanday sonlar tub sonlar deb yuritiladi?	*Faqatgina 1 ga va o’ziga bo’linadigan sonlar

		tub sonlar deyiladi.
711.	To‘liq zaxiralash	Tiklashning tezligi yuqori. axira nusxalash jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi
712.	O‘sib boruvchi zaxiralash	Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi
713.	Differnsial zaxiralash	Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi
714.	Ushbu jarayon ma’lumot qanday yo‘qolgani, ma’lumotni qayta tiklash dasturiy vositasi va ma’lumotni tiklash anzilini qayergaligiga bog‘liq bo‘ladi. Qaysi jarayon	Ma’lumotlarni qayta tiklash
715.	Antivirus dasturlarini ko’rsating?	*Drweb, Nod32, Kaspersky
716.	Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi	*wep, wpa, wpa2
717.	Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak?	*ishonchli, qimmatli va to’liq
718.	Axborotning eng kichik o’lchov birligi nima?	*bit
719.	Virtual xususiy tarmoq – bu?	*VPN
720.	Xavfli viruslar bu - …	*kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar
721.	Mantiqiy bomba – bu …	*Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari
722.	Rezident virus...	*tezkor xotirada saqlanadi
723.	DIR viruslari nimani zararlaydi?	*FAT tarkibini zararlaydi
724.	.... kompyuter tarmoqlari bo’yicha tarqalib, kompyuterning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi	*«Chuvalchang» va replikatorli virus
725.	Mutant virus...	*shifrlash va deshifrlash algoritmlaridan iborat
726.	Fire Wall ning vazifasi...	*tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi
727.	Kompyuter virusi nima?	*maxsus yozilgan va zararli dastur
728.	Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating	*disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali
729.	Troyan dasturlari bu...	*virus dasturlar
730.	Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi?	*5
731.	Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud	*detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar
732.	Axborotni himoyalash uchun ... usullari qo’llaniladi.	*kodlashtirish, kriptografiya, stegonografiya
733.	Stenografiya mahnosi...	*sirli yozuv
734.	…sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi	*K.Shennon
735.	Kriptologiya yo’nalishlari nechta?	*2
736.	Kriptografiyaning asosiy maqsadi...	*maxfiylik, yaxlitlilikni ta`minlash
737.	Zararli dasturiy vositalarni aniqlash turlari nechta	*3

738.	Signaiurana asoslangan	*....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin.
739.	O‘zgarishni aniqlashga asoslangan	....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin.
740.	Anomaliyaga asoslangan	....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin.
741.	Antiairuslar qanday usulda viruslarni aniqlaydi	Anomaliyaga asoslangan
742.	Viruslar -	bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi
743.	Rootkitlar-	bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi
744.	Backdoorlar -	bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vositasifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi
745.	Troyan otlari-	*bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi
746.	Ransomware-	bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi
747.	Resurslardan foydalanish usuliga ko’ra viruslar qanday turlarga bo’linadi	*Virus parazit, Virus cherv
748.	Zararlagan obyektlar turiga ko’ra	Virus parazit, Virus cherv
749.	Faollashish prinspiga ko’ra	Virus parazit, Virus cherv
750.	Dastur kodini tashkil qilish yondashuviga ko‘ra	Virus parazit, Virus cherv
751.	Shifrlanmagan viruslar	*o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi.
752.	Shifrlangan viruslar	o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi.
753.	Polimorf viruslar	o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi.
754.	Dasturiy viruslar-…	bir vaqtning o‘zida turli xildagi Obyektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi.

755.	Ko‘p platformali viruslar	*bir vaqtning o‘zida turli xildagi Obyektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi.
756.	Yuklanuvchi viruslar	bir vaqtning o‘zida turli xildagi Obyektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi.
757.	Makroviruslar-...	bir vaqtning o‘zida turli xildagi Obyektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi.
758.	Birinchi kompyuter virusi nima deb nomlangan	Cherv
759.	P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang	*840
760.	256mod25=?	5
761.	bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi.	*Tizim
762.	Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori satxli hujjat yoki hujjatlar to‘plami nima duyidadi	Standart
763.	RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday?	65535;
764.	DES algoritmi akslantirishlari raundlari soni qancha?	*16;
765.	DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha?	CHap qism blok 32 bit, o‘ng qism blok 48 bit;
766.	Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor?	SHifrlash va deshifrlash jarayonlarida kalitlardan foydalanish qoidalariga ko‘ra farqlanadi
767.	19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta?	19 ta
768.	10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta?	*4 ta
769.	Qaysi formula qoldiqli bo’lish qonunini ifodalaydi	$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$
770.	Eyler funsiyasida $\phi(1)$ qiymati nimaga teng?	*0
771.	Eyler funksiyasida 60 sonining qiymatini toping.	59
772.	Eyler funksiyasi yordamida 1811 sonining qiymatini toping.	*1810
773.	97 tub sonmi?	*Tub
774.	Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256.	*244

775.	Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220	21
776.	Quyidagi ifodani qiymatini toping. -17mod11	6
777.	2 soniga 10 modul bo’yicha teskari sonni toping.	3

778. I:
779. S: Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.
780. +: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik
781. -: Axborot va Iqtisodiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xafvsizligi, Dasturiy ta`minot xavfsizligi
782. -: Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xafvsizligi, Ekologik xavfsizlik
783. -: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Dasturiy ta`minot xavfsizligi, Ekologik xavfsizlik
784. I:
785. S: Axborot xavfsizligining asosiy maqsadlaridan biri- bu…
786. +: Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish
787. -:Ob`yektga bevosita ta`sir qilish
788. -: Axborotlarni shifrlash, saqlash, yetkazib berish
789. -: Tarmoqdagi foydalanuvchilarni xavfsizligini ta`minlab berish
790. I:
791. S: Konfidentsiallikga to’g’ri ta`rif keltiring.
792. +: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
793. -:axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati;
794. -:axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati;
795. -:axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati;
796. I:
797. S: Yaxlitlikni buzilishi bu - …
798. +: Soxtalashtirish va o’zgartirish
799. -: Ishonchsizlik va soxtalashtirish
800. -: Soxtalashtirish
801. -: Butunmaslik va yaxlitlanmaganlik
802. I:
803. S:... axborotni himoyalash tizimi deyiladi.
804. +: Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi
805. -: Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo’qotilishidan keladigan zarar va himoyalash mexanizmining narxidan kelib chiqqan holda axborotni himoyalashning zaruriy darajasi
806. -: Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo’qotilishidan keladigan zarar va himoyalash mexanizmining zaruriy darajasi hamda tizimning turini, himoyalash usullar va vositalari

-: Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo'qotilishiga to'sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul

I:

S: Kompyuter virusi nima?

+: maxsus yozilgan va zararli dastur

-:.exe fayl

-: boshqariluvchi dastur

-: Kengaytmaga ega bo'lgan fayl

I:

S: Kriptografiyaning asosiy maqsadi...

+: maxfiylik, yaxlitlilikni ta`minlash

-:ishonchlilik, butunlilikni ta`minlash

-:autentifikatsiya, identifikatsiya

-:ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya

I:

S: SMTP - Simple Mail Transfer protokol nima?

+: elektron pochta protokoli

-:transport protokoli

-:internet protokoli

-:Internetda ommaviy tus olgan dastur

I:

S: SKIP protokoli...

+: Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi

-:Protokollar boshqaruvi

-:E-mail protokoli

-:Lokal tarmoq protokollari uchun kriptokalitlarning oddiy boshqaruvi

I:

S: Kompyuter tarmog'ining asosiy komponentlariga nisbatan xavf-xatarlar…

+: uzilish, tutib qolish, o'zgartirish, soxtalashtirish

-:o'zgartirish, soxtalashtirish

-:tutib qolish, o'zgarish, uzilish

-:soxtalashtirish, uzilish, o'zgartirish

I:

S: ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.

+: konfidentsiallik

-:identifikatsiya

-:autentifikatsiya

-: maxfiylik

I:

S: Foydalanish huquqini cheklovchi matritsa modeli bu...

+: Bella La-Padulla modeli

-:Dening modeli

-:Landver modeli

-:Huquqlarni cheklovchi model

I:

851. S: Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi?
852. +: TCP/IP, X.25 protokollar
853. -:X.25 protokollar
854. -:TCP/IP
855. -:SMTP
856. I:
857. S: Autentifikatsiya nima?
858. +: Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi
859. -: Tizim meyoriy va g’ayritabiiy hollarda rejalashtirilgandek o’zini tutishligi holati
860. -: Istalgan vaqtda dastur majmuasining mumkinligini kafolati
861. -:Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi
862. I:
863. S:Identifikatsiya bu- …
864. +: Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni
865. -:Ishonchliligini tarqalishi mumkin emasligi kafolati
866. -:Axborot boshlang’ich ko’rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o’zgarishlar
867. -:Axborotni butunligini saqlab qolgan holda uni elementlarini o’zgartirishga yo’l qo’ymaslik
868. I:
869. S:O’rin almashtirish shifri bu - …
870. +: Murakkab bo’lmagan kriptografik akslantirish
871. -:Kalit asosida generatsiya qilish
872. -:Ketma-ket ochiq matnni ustiga qo’yish
873. -:Belgilangan biror uzunliklarga bo’lib chiqib shifrlash
874. I:
875. S:Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.
876. +: 2 turga
877. -:3 turga
878. -:4 turga
879. -: 5 turga
880. I:
881. S: Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular …
882. +: hosil qilish, yig’ish, taqsimlash
883. -:ishonchliligi, maxfiyligi, aniqligi
884. -:xavfsizlik, tez ishlashi, to’g’ri taqsimlanishi
885. -:abonentlar soni, xavfsizligi, maxfiyligi
886. I:
887. S: Kriptologiya -
888. +: axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
889. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
890. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi

-:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

I:

S: Kriptografiyada alifbo –

+: axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam

-:matnni shifrlash va shifrini ochish uchun kerakli axborot

-:xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha

-:kalit axborotni shifrlovchi kalitlar

I:

S: Simmetrik kriptotizimlarda ... jumlani davom ettiring

+: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi

-:bir-biriga matematik usullar bilan bog’langan ochiq va yopiq kalitlardan foydalaniladi

-:axborot ochiq kalit yordamida shifrlanadi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi

-:kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi

I:

S: Kriptobardoshlilik deb …

+: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

-:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi

-:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi

-:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

I:

S: Elektron raqamli imzo deb –

+: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha

-:matnni shifrlash va shifrini ochish uchun kerakli axborot

-:axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam

-:kalit axborotni shifrlovchi kalitlar

I:

S: Kriptografiya –

+: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

-:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi

-:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi

-:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

I:

S: Kriptografiyada matn –

+: alifbo elementlarining tartiblangan to’plami

-:matnni shifrlash va shifrini ochish uchun kerakli axborot

-:axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam

-:kalit axborotni shifrlovchi kalitlar

I:

929. S: Kriptoanaliz –
930. +: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
931. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
932. -:axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi
933. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o'rganadi
934. I:
935. S: Shifrlash –
936. +: akslantirish jarayoni ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi
937. -:kalit asosida shifrmatn ochiq matnga akslantiriladi
938. -:shifrlashga teskari jarayon
939. -:Almashtirish jarayoni bo'lib: ochiq matn deb nomlanadigan matn o'girilgan holatga almashtiriladi
940. I:
941. S: Faol hujum turi deb…
942. +: Maxfiy uzatish jarayonini uzib qo'yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon
943. -:Maxfiy ma`lumotni aloqa tarmog'ida uzatilayotganda eshitish, tahrir qilish, yozib olish harakatlaridan iborat uzatilalayotgan ma`lumotni qabul qiluvchiga o'zgartirishsiz yetkazish jarayoni
944. -:Ma`lumotga o'zgartirish kiritmay uni kuzatish jarayoni
945. -:Sust hujumdan farq qilmaydigan jarayon
946. I:
947. S: Blokli shifrlash-
948. +: shifrlanadigan matn blokiga qo'llaniladigan asosiy akslantirish
949. -:murakkab bo'lmagan kriptografik akslantirish
950. -:axborot simvollarini boshqa alfavit simvollari bilan almashtirish
951. -:ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi
952. I:
953. S: Simmetrik kriptotizmning uzluksiz tizimida …
954. +: ochiq matnning har bir harfi va simvoli alohida shifrlanadi
955. -:belgilangan biror uzunliklarga teng bo'linib chiqib shifrlanadi
956. -:murakkab bo'lmagan kriptografik akslantirish orqali shifrlanadi
957. -:ketma-ket ochiq matnlarni o'rniga qo'yish orqali shifrlanadi
958. I:
959. S: Kriptotizimga qo'yiladigan umumiy talablardan biri
960. +: shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak
961. -:shifrlash algoritmining tarkibiy elementlarini o'zgartirish imkoniyati bo'lishi lozim
962. -:ketma-ket qo'llaniladigan kalitlar o'rtasida oddiy va oson bog'liqlik bo'lishi kerak
963. -:maxfiylik o'ta yuqori darajada bo'lmoqligi lozim
964. I:
965. S: Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?
966. +: Asimmetrik kriptotizimlarda k1≠k2 bo'lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

967. -:Asimmetrik tizimlarda k1=k2 bo’ladi, yahni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi
968. -:Asimmetrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma`lum bo’ladi, ochiq kalitni esa faqat qabul qiluvchi biladi
969. -:Asimmetrik kriptotizimlarda k1≠k2 bo’lib, kalitlar hammaga oshkor etiladi
970. I:
971. S: Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang
972. +: Vijener matritsasi, Sezar usuli
973. -:monoalfavitli almashtirish
974. -:polialfavitli almashtirish
975. -:o’rin almashtirish
976. I:
977. S: Akslantirish tushunchasi deb nimaga aytiladi?
978. +: 1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga
979. -:1-to’plamli elementlariga 2-to’plam elementalrini qarama-qarshiligiga
980. -:har bir elementni o’ziga ko’payimasiga
981. -:agar birinchi va ikinchi to’plam bir qiymatga ega bulmasa
982. I:
983. S: Simmetrik guruh deb nimaga aytiladi?
984. +: O’rin almashtirish va joylashtirish
985. -:O’rin almashtirish va solishtirish
986. -:Joylashtirish va solishtirish
987. -:O’rin almashtirish va transportizatsiyalash
988. I:
989. S: Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?
990. +: simmetrik kriptosistemalar
991. -:assimetrik kriptosistemalar
992. -:ochiq kalitli kriptosistemalar
993. -:autentifikatsiyalash
994. I:
995. S: Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?
996. +: SMTP, POP yoki IMAP
997. -:SKIP, ATM, FDDI
998. -:X.25 va IMAR
999. -:SMTP, TCP/IP
1000. I:
1001. S: Axborot resursi – bu?
1002. +: axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi
1003. -:cheklanmagan doiradagi shaxslar uchun mo’ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar
1004. -:identifikatsiya qilish imkonini beruvchi rekvizitlari qo’yilgan holda moddiy jismda qayd etilgan axborot

1005. -:manbalari va taqdim etilish shaklidan qathi nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to’g’risidagi ma`lumotlar
1006. I:
1007. S: Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu?
1008. +: login parol
1009. -:identifikatsiya
1010. -:maxfiy maydon
1011. -: token
1012. I:
1013. S: Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu?
1014. +: parol
1015. -:login
1016. -:identifikatsiya
1017. -:maxfiy maydon foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
1018. I:
1019. S: Identifikatsiya jarayoni qanday jarayon?
1020. +: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
1021. -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
1022. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
1023. -:foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
1024. I:
1025. S: Autentifikatsiya jarayoni qanday jarayon?
1026. +: obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
1027. -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
1028. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
1029. -:foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
1030. I:
1031. S: Ro’yxatdan o’tish bu?
1032. +: foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
1033. -:axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
1034. -:ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash

-:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

I:

S: Axborot qanday sifatlarga ega bo’lishi kerak?

+: ishonchli, qimmatli va to’liq

-:uzluksiz va uzlukli

-:ishonchli, qimmatli va uzlukli

-:ishonchli, qimmatli va uzluksiz

I:

S: Axborotning eng kichik o’lchov birligi nima?

+: bit

-:kilobayt

-:bayt

-:bitta simvol

I:

S: Elektron hujjatning rekvizitlari nechta qismdan iborat?

+: 4

-:5

-:6

-:7

I:

S: Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?

+: fleshka, CD va DVD disklar

-:Qattiq disklar va CDROM

-:CD va DVD, DVDROM

-:Qattiq disklar va DVDROM

I:

S: Avtorizatsiya jarayoni qanday jarayon?

+: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

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

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

-: parollash jarayoni

I:

S: Kodlash nima?

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

-:Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi

mumkin bo‘ladi

-:Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi

mumkin bo‘ladi

-:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi

1074. I:
1075. S: Shifrlash nima?
1076. +: Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi
1077. -:Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir
1078. -: Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi
1079. -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi
1080. I:
1081. S: Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi
1082. +:Kriptoanaliz
1083. -:Kartografiya
1084. -:Kriptologiya
1085. -:Adamar usuli
1086. I:
1087. S: Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi
1088. +: {d, n} – yopiq, {e, n} – ochiq;
1089. -:{d, e} – ochiq, {e, n} – yopiq;
1090. -:{e, n} – yopiq, {d, n} – ochiq;
1091. -:{e, n} – ochiq, {d, n} – yopiq;
1092. I:
1093. S: Zamonaviy kriptografiya qanday bo’limlardan iborat?
1094. -:Electron raqamli imzo; kalitlarni boshqarish
1095. -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;
1096. +: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish
1097. -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; kalitlarni boshqarish
1098. I:
1099. S: Shifr nima?
1100. +: Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm
1101. -:Kalitlarni taqsimlash usuli
1102. -:Kalitlarni boshqarish usuli
1103. -:Kalitlarni generatsiya qilish usuli
1104. I:
1105. S: Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?
1106. +: Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi
1107. -:Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi
1108. -:Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin
1109. -:Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat deshifrlash mumkin
1110. I:
1111. S: Oqimli shifrlashning mohiyati nimada?
1112. +: Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,

1113. -:Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur,
1114. -:Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi
1115. -:Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,
1116. I:
1117. S: Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating.
1118. +: uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim,
1119. -:uzatilayotgan xabarni xavfsizligi kalitni maxfiyligiga emas, balki algoritmni maxfiyligiga bog’liq bo’lishi lozim
1120. -:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog’liq bo’lishi lozim
1121. -:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga emas, balki shifrlashda foydalaniladigan arifmetik amallar soniga bog’liq bo’lishi lozim
1122. I:
1123. S: Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?
1124. +: shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun
1125. -:ERI yaratish va tekshirish, kalitlar almashish uchun
1126. -:shifrlash, deshifrlash, kalitlar almashish uchun
1127. -: Heshlash uchun
1128. I:
1129. S: Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi.
1130. +: ochiq kalitlar
1131. -:yopiq kalitlar
1132. -:seans kalitlari
1133. -:Barcha tutdagi kalitlar
1134. I:
1135. S: Kompyuterning tashqi interfeysi deganda nima tushuniladi?
1136. +: kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari
1137. -:tashqi qurilmani kompyuterga bog’lashda ishlatiladigan ulovchi simlar
1138. -:kompyuterning tashqi portlari.
1139. -:tashqi qurilma bilan kompyuter o’rtasida axborot almashinish qoidalari to’plami
1140. I:
1141. S: Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?
1142. +: Yulduz
1143. -:Xalqa
1144. -:To’liqbog’langan
1145. -:Umumiy shina
1146. I:
1147. S: Ethernet kontsentratori qanday vazifani bajaradi

+: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi

-:kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo’naltirib beradi

-:kompyuterdan kelayotgan axborotni xalqa bo’ylab joylashgan keyingi kompyuterga

-:tarmoqning ikki segmentini bir biriga ulaydi

I:

S: OSI modelida nechta satx mavjud

+: 7

-:4

-:5

-:3

I:

S: OSI modelining to’rtinchi satxi qanday nomlanadi

+: Transport satxi

-:Amaliy satx

-:Seanslar satxi

-:Taqdimlash satxi

I:

S: OSI modelining beshinchi satxi qanday nomlanadi

+: Seanslar satxi

-:Tarmoq satxi

-:Fizik satx

-:Amaliy satx

I:

S: OSI modelining birinchi satxi qanday nomlanadi

+: Fizik satx

-:Seanslar satxi

-:Transport satxi

-:Taqdimlash satxi

I:

S: OSI modelining ikkinchi satxi qanday nomlanadi

+: Kanal satxi

-:Amaliy satxi

-:Fizik satx

-:Seanslar satxi

I:

S: OSI modelining uchinchi satxi qanday nomlanadi

+: Tarmoq satxi

-:Amaliy satx

-:Kanal satxi

-:Taqdimlash satxi

I:

S: OSI modelining oltinchi satxi qanday nomlanadi

+: Taqdimlash satxi

-:Amaliy satx

-:Seanslar satxi

1193. -:Kanal satxi
1194. I:
1195. S: OSI modelining yettinchi satxi qanday nomlanadi
1196. +: Amaliy satx
1197. -:Seanslar satxi
1198. -:Transport satxi
1199. -:Taqdimlash satxi
1200. I:
1201. S: OSI modelining qaysi satxlari tarmoqqa bog'liq satxlar hisoblanadi
1202. +: fizik, kanal va tarmoq satxlari
1203. -:seans va amaliy satxlar
1204. -:amaliy va taqdimlash satxlari
1205. -:transport va seans satxlari
1206. I:
1207. S: OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi
1208. +: Marshrutizator
1209. -:Ko'prik
1210. -:Tarmoq adapter
1211. -:Kontsentrator
1212. I:
1213. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
1214. +: Fizik satx
1215. -:Kanal satxi
1216. -:Tarmoq satxi
1217. -:Transport satxi
1218. I:
1219. S: Ma'lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi
1220. +: Tarmoq satxi
1221. -:Kanal satxi
1222. -:Amaliy satx
1223. -:Transport satxi
1224. I:
1225. S: Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub
1226. +: IP, IPX
1227. -:NFS, FTP
1228. -:Ethernet, FDDI
1229. -:TCP,UDP
1230. I:
1231. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
1232. +: TCP,UDP
1233. -:NFS, FTP
1234. -:IP, IPX
1235. -:Ethernet, FDDI
1236. I:

1237. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
1238. +: Elektr signallarini uzatish va qabul qilish
1239. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojaat qilishni boshqarish
1240. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
1241. -:Klient dasturlari bilan o’zaro muloqotda bo’lish
1242. I:
1243. S: Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...
1244. +: Avtorizatsiya
1245. -:Shifrlash
1246. -:Identifikatsiya
1247. -:Autentifikatsiya
1248. I:
1249. S: Autentifikatsiya faktorlari nechta
1250. +: 3
1251. -:4
1252. -:5
1253. -: 6
1254. I:
1255. S: Ko‘z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar?
1256. +: Biometrik autentifikatsiya
1257. -:Biron nimaga egalik asosida
1258. -:Biron nimani bilish asosida
1259. -:Parolga asoslangan
1260. I:
1261. S: Barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi?
1262. +: Fizik satx
1263. -:Tarmoq satxi
1264. -:Amaliy satx
1265. -:Tadbiqiy sath
1266. I:
1267. S: Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi
1268. +: 2
1269. -:4
1270. -:3
1271. -:5
1272. I:
1273. S: Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?
1274. +: Subyekt
1275. -:Obyekt
1276. -:Tizim
1277. -:Jarayon
1278. I:

1279. S: MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi
1280. +: xavfsizlik siyosati ma’muri
1281. -:Foydalaguvchining o‘zi
1282. -:Dastur tomonidan
1283. -:Boshqarish amaalga oshirilmaydi
1284. I:
1285. S: Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi
1286. +: O‘qish
1287. -:Yozish
1288. -:O‘zgartirish
1289. -:Yashirish
1290. I:
1291. S: Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.
1292. +: Yozish
1293. -:O‘qish
1294. -:O‘zgartirish
1295. -:Yashirish
1296. I:
1297. S: Rol tushunchasiga ta’rif bering.
1298. +: Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin
1299. -:Foydalanishni boshqarish
1300. -:Muayyan faoliyat turi bilan bog‘liq imkoniyatlar to‘plami sifatida belgilanishi mumkin
1301. -:Vakolitlarni taqsimlash
1302. I:
1303. S: Foydalanishni boshqarishning qaysi usuli - Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.
1304. +: ABAC
1305. -:MAC
1306. -:DAC
1307. -:RBAC
1308. I:
1309. S: Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?
1310. +: barchasi
1311. -:bimetrik alomatlarning ishga layoqatli shaxsdan ajratib bo‘lmasligi
1312. -:biometrik alomatlarni soxtalashtirishning qiyinligi
1313. -:biometrik alomatlarni noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasi yuqoriligi
1314. I:
1315. S: OSI modeli 7 satxi bu
1316. +: Ilova
1317. -:Seans

-:Fizik
-:Kanal
I:
S: OSI modeli 1 satxi bu
+: Fizik
-:Ilova
-:Seans
-:Kanal
I:
S: OSI modeli 2 satxi bu
+:Kanal
-: Fizik
-:Ilova
-:Seans
I:
S: TCP/IP modelida nechta satx mavjud
+: 4
-:3
-:2
-:8
I:
S: Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi?
+: Shaxsiy tarmoq
-:Lokal
-:Mintaqaviy
-:CAMPUS
I:
S: Tarmoq kartasi bu...
+: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
-:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.
-: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.
I:
S: Server xotirasidagi joyni bepul yoki pulli ijagara berish xizmati qanday ataladi?

+: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
-:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
-:Signalni tiklash yoki qaytarish uchun foydalaniladi.
-:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.

1356. I:
1357. S: Hab bu...
1358. +: ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
1359. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
1360. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.
1361. -:qabul qilingan signalni barchachiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
1362. I:
1363. S: Tarmoq repiteri bu...
1364. +: Signalni tiklash yoki qaytarish uchun foydalaniladi.
1365. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
1366. -:ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
1367. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
1368. I:
1369. S: Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi.
1370. +: DNS tizimlari
1371. -:TCP/IP
1372. -:Ethernet
1373. -:Token ring
1374. I:
1375. S: ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.
1376. +: TCP
1377. -:IP
1378. -:HTTP
1379. -:FTP
1380. I:
1381. S: …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.
1382. +: UDP
1383. -:HTTP
1384. -:TCP
1385. -:FTP
1386. I:
1387. S: Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi.
1388. +: IP
1389. -:TCP
1390. -:HTTP
1391. -:FTP

1392. I:
1393. S: Tarmoq taxdidlari necha turga bo‘linadi
1394. +: 4
1395. -:2
1396. -:3
1397. -:5
1398. I:
1399. S: Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;
1400. +: Razvedka hujumlari
1401. -:Kirish hujumlari
1402. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
1403. -:Zararli hujumlar
1404. I:
1405. S: Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi
1406. +: Kirish hujumlari
1407. -:Razvedka hujumlari
1408. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
1409. -:Zararli hujumlar
1410. I:
1411. S: Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;
1412. +: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
1413. -:Razvedka hujumlari
1414. -:Kirish hujumlari
1415. -:Zararli hujumlar
1416. I:
1417. S: Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;
1418. +: Zararli hujumlar
1419. -:Razvedka hujumlari
1420. -:Kirish hujumlari
1421. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
1422. I:
1423. S: RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart?
1424. +: e soni Eyler funksiyasi - $\varphi(n)$ bilan o‘zaro tub
1425. -:e ning qiymati [1,n] kesmaga tegishli ixtiyoriy son
1426. -:e soni ixtiyoriy tub son
1427. -:e soni ixtiyoriy butun musbat son
1428. I:
1429. S: RSA elektron raqamli imzo algoritmidagi yopiq kalit d qanday hisoblanadi? Bu yerda p va q tub sonlar,n=pq, $\varphi(n)$- Eyler funksiyasi,e-ochiq kalit
1430. +: $d = e^{-1} mod \varphi(n)$
1431. -: $d = e^{-1} mod q$
1432. -:$d = e^{-1} mod q$
1433. -:$d = e^{-1} mod p$

1434. I:
1435. S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?
1436. +: Imzo qo‘yish va imzoni tekshirishdan
1437. -:Faqat imzo qo‘yishdan
1438. -:Faqat imzoni tekshirishdan

1439. -:Barcha javoblar to‘g‘ri
1440. I:
1441. S: Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi?
1442. +: Imzo muallifining ochiq kaliti yordamida
1443. -:Ma’lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida
1444. -:Ma’lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida
1445. -:Imzo muallifining maxfiy kaliti yordamida
1446. I:
1447. S: Tarmoq modeli-bu...
1448. +: Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir
1449. -:Global tarmoq qurish usullari
1450. -:Lokal tarmoq qurish usullari
1451. -:To‘g‘ri javob yo‘q.
1452. I:
1453. S: OSI modeli nechta satxga ajraladi?
1454. +: 7
1455. -:2
1456. -:4
1457. -:3
1458. I:
1459. S: TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi
1460. +: Kanal, Fizik
1461. -:Tarmoq
1462. -:Tramsport
1463. -:Ilova, taqdimot, seans.
1464. I:
1465. S: TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi
1466. +: Tarmoq
1467. -:Kanal, Fizik
1468. -:Tramsport
1469. -:Ilova, taqdimot, seans.
1470. I:
1471. S: TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi
1472. +: Tramsport
1473. -:Kanal, Fizik
1474. -:Tarmoq
1475. -:Ilova, taqdimot, seans.
1476. I:

1477. S: TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos keladi
1478. +: Ilova, taqdimot, seans
1479. -:Kanal, Fizik
1480. -:Tarmoq
1481. -:Tramsport
1482. I:
1483. S: Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.
1484. +: Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
1485. -:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
1486. -:Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi
1487. -:Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi
1488. I:
1489. S: Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.
1490. +: Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
1491. -:Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
1492. -:Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi
1493. -:Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi.
1494. I:
1495. S: Repetir nima?
1496. +: Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
1497. -:Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
1498. -: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
1499. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
1500. I:
1501. S: Hub nima?
1502. +: Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
1503. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi, Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
1504. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
1505. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
1506. I:

1507. S: Router nima?
1508. +: Qabul qilingan ma’lumotlarni tarmoq satxiga tegishli manzillarga ko‘ra (IP manzil) uzatadi.
1509. -:Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
1510. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
1511. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
1512. I:
1513. S: Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi
1514. +: Razvedka hujumlari
1515. -:Kirish hujumlari
1516. -:DOS hujumi
1517. -:Zararli hujumlar
1518. I:
1519. S: Razvedka hujumiga berilgan ta’rifni aniqlang
1520. +: Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;
1521. -:hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi hujumchi -:mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;
1522. -:zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;
1523. I:
1524. S: OSI modelining birinchi satxi qanday nomlanadi
1525. +: Fizik satx
1526. -:Seanslar satxi
1527. -:Transport satxi
1528. -:Taqdimlash satxi
1529. I:
1530. S: OSI modelining ikkinchi satxi qanday nomlanadi
1531. +: Kanal satxi
1532. -:Amaliy satxi
1533. -:Fizik satx
1534. -:Seanslar satxi
1535. I:
1536. S: OSI modelining uchinchi satxi qanday nomlanadi
1537. +: Tarmoq satxi
1538. -:Amaliy satx
1539. -:Kanal satxi
1540. -:Taqdimlash satxi
1541. I:
1542. S: OSI modelining oltinchi satxi qanday nomlanadi
1543. +: Taqdimlash satxi
1544. -:Amaliy satx
1545. -:Seanslar satxi

-:Kanal satxi
I:
S: OSI modelining ettinchi satxi qanday nomlanadi
+: Amaliy satx
-:Seanslar satxi
-:Transport satxi
-:Taqdimlash satxi
I:
S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
+: Fizik satx
-:Kanal satxi
-:Tarmoq satxi
-:Transport satxi
I:
S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
+: TCP,UDP
-:NFS, FTP
-:IP, IPX
-:Ethernet, FDDI
I:
S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
+: Elektr signallarini uzatish va qabul qilish
-:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
-:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
-:Klient dasturlari bilan o’zaro muloqotda bo’lish
I:
S: OSI modelining amaliy satxi qanday funksiyalarni bajaradi
+: Klient dasturlari bilan o’zaro muloqotda bo’lish
-:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
-:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
-:Elektr signallariniuzatish va qabul qilish
I:
S: Yevklid algoritmi qanday natijani beradi?
+: Sonning eng katta umumiy bo’luvchisini toppish
-:Sonning turli bo’luvchilarini toppish
-:Sonning eng kichik umumiy karralisini toppish
-:Sonning eng katta umumiy bo’linuvchisini topish
I:
S: Qanday sonlar tub sonlar deb yuritiladi?
+: Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi.
-:O’zidan boshqa bo’luvchilari mavjud bo’lgan sonlar tub sonlar deyiladi.
-:Agar sonning 1 dan boshqa bo’luvchilari bo’lsa.
-:Faqatgina 1 ga o’ziga bo’linmaydigan sonlar tub sonlar deyiladi.
I:

1590. S: OSI modelining birinchi satxi qanday nomlanadi
1591. +: Fizik satx
1592. -:Seanslar satxi
1593. -:Transport satxi
1594. -:Taqdimlash satxi
1595. I:
1596. S: OSI modelining ikkinchi satxi qanday nomlanadi
1597. +: Kanal satxi
1598. -:Amaliy satxi
1599. -:Fizik satx
1600. -:Seanslar satxi
1601. I:
1602. S: OSI modelining uchinchi satxi qanday nomlanadi
1603. +: Tarmoq satxi
1604. -:Amaliy satx
1605. -:Kanal satxi
1606. -:Taqdimlash satxi
1607. I:
1608. S: OSI modelining oltinchi satxi qanday nomlanadi
1609. +: Taqdimlash satxi
1610. -:Amaliy satx
1611. -:Seanslar satxi
1612. -:Kanal satxi
1613. I:
1614. S: OSI modelining ettinchi satxi qanday nomlanadi
1615. +: Amaliy satx
1616. -:Seanslar satxi
1617. -:Transport satxi
1618. -:Taqdimlash satxi
1619. I:
1620. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
1621. +: Fizik satx
1622. -:Kanal satxi
1623. -:Tarmoq satxi
1624. -:Transport satxi
1625. I:
1626. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
1627. +: TCP,UDP
1628. -:NFS, FTP
1629. -:IP, IPX
1630. -:Ethernet, FDDI
1631. I:
1632. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
1633. +: Elektr signallarini uzatish va qabul qilish
1634. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish

-:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
-:Klient dasturlari bilan o’zaro muloqotda bo’lish
I:
S: OSI modeliningamaliy satxi qanday funktsiyalarni bajaradi
+: Klient dasturlari bilan o’zaro muloqotda bo’lish
-:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
-:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
-:Elektr signallariniuzatish va qabul qilish
I:
S: Yevklid algoritmi qanday natijani beradi?
+: Sonning eng katta umumiy bo’luvchisini toppish
-:Sonning turli bo’luvchilarini toppish
-:Sonning eng kichik umumiy karralisini toppish
-:Sonning eng katta umumiy bo’linuvchisini topish
I:
S: Qanday sonlar tub sonlar deb yuritiladi?
+: Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi.
-:O’zidan boshqa bo’luvchilari mavjud bo’lgan sonlar tub sonlar deyiladi.
-:Agar sonning 1 dan boshqa bo’luvchilari bo’lsa.
-:Faqatgina 1 ga o’ziga bo’linmaydigan sonlar tub sonlar deyiladi.
I:
S: Antivirus dasturlarini ko’rsating?
+: Drweb, Nod32, Kaspersky
-:arj, rar, pkzip, pkunzip
-:winrar, winzip, winarj
-:pak, lha
I:
S: Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi
+: wep, wpa, wpa2
-:web, wpa, wpa2
-:wpa, wpa2
-:wpa, wpa2, wap
I:
S: Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak?
+: ishonchli, qimmatli va to’liq
-:uzluksiz va uzlukli
-:ishonchli, qimmatli va uzlukli
-:ishonchli, qimmatli va uzluksiz
I:
S: Axborotning eng kichik o’lchov birligi nima?
+: bit
-:kilobayt
-:bayt
-:bitta simvol
I:
S: Virtual xususiy tarmoq – bu?

1681. +: VPN
1682. -:APN
1683. -:ATM
1684. -:Ad-hoc
1685. I:
1686. S: Xavfli viruslar bu - …
1687. +: kompyuter ishlashida jiddiy nuqsonlarga sabab bo'luvchi viruslar
1688. -:tizimda mavjudligi turli taassurot (ovoz, video) bilan bog'liq viruslar, bo'sh xotirani kamaytirsada, dastur va ma`lumotlarga ziyon yetkazmaydi
1689. -:o'z-o'zidan tarqalish mexanizmi amalga oshiriluvchi viruslar
1690. -:dastur va ma`lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o'chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar
1691. I:
1692. S: Mantiqiy bomba – bu …
1693. +: Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari
1694. -:Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari
1695. -:Viruslar kodiga boshqarishni uzatish
1696. -:Qidirishning passiv mexanizmlarini amalga oshiruvchi, yahni dasturiy fayllarga tuzoq qo'yuvchi viruslar
1697. I:
1698. S: Rezident virus...
1699. +: tezkor xotirada saqlanadi
1700. -:to'liqligicha bajarilayotgan faylda joylashadi
1701. -:ixtiyoriy sektorlarda joylashgan bo'ladi
1702. -:alohida joyda joylashadi
1703. I:
1704. S: DIR viruslari nimani zararlaydi?
1705. +: FAT tarkibini zararlaydi
1706. -:com, exe kabi turli fayllarni zararlaydi
1707. -:yuklovchi dasturlarni zararlaydi
1708. -:Operatsion tizimdagi sonfig.sys faylni zararlaydi
1709. I:
1710. S:.... kompyuter tarmoqlari bo'yicha tarqalib, komlg'yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o'zining nusxasini qoldiradi
1711. +: «Chuvalchang» va replikatorli virus
1712. -:Kvazivirus va troyan virus
1713. -:Troyan dasturi
1714. -:Mantiqiy bomba
1715. I:
1716. S: Fire Wall ning vazifasi...
1717. +: tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta`minlaydi
1718. -:kompyuterlar tizimi xavfsizligini ta`minlaydi
1719. -:Ikkita kompyuter o'rtasida aloqa o'rnatish jarayonida Internet tarmog'i orasida xavfsizlikni ta`minlaydi

-:uy tarmog’i orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi
I:
S: Kompyuter virusi nima?
+: maxsus yozilgan va zararli dastur
-:.exe fayl
-:boshqariluvchi dastur
-:Kengaytmaga ega bo’lgan fayl
I:
S: Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating
+: disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali
-: faqat maxsus tashuvchi qurilma orqali
-: faqat kompyuter tarmoqlari orqali
-:zararlanish yo’llari juda ko’p
I:
S: Troyan dasturlari bu...
+: virus dasturlar
-:antivirus dasturlar
-:o’yin dasturlari
-:yangilovchi dasturlar
I:
S: Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi?
+: 5
-:4
-:2
-:3
I:
S: Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud
+: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar
-:detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar
-:vaktsinalar, privivkalar, revizorlar, tekshiruvchilar
-:privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar
I:
S: Stenografiya mahnosi...
+: sirli yozuv
-:sirli xat
-:maxfiy axborot
-:maxfiy belgi
I:
S: …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi
+: K.Shennon
-:Sezar
-:U.Xill
-:Fon Neyman
I:
S: Kriptologiya yo’nalishlari nechta?
+: 2

-:3
-:4
-:5
I:
S: Kriptografiyaning asosiy maqsadi...
+: maxfiylik, yaxlitlilikni ta`minlash
-:ishonchlilik, butunlilikni ta`minlash
-:autentifikatsiya, identifikatsiya
-:ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya
I:
S: DES algoritmi akslantirishlari raundlari soni qancha?
+: 16;
-:14;
-:12;
-:32;
I:
S: DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha?
+: CHap qism blok 32 bit, o‘ng qism blok 32 bit;
-:CHap qism blok 32 bit, o‘ng qism blok 48 bit;
-:CHap qism blok 64 bit, o‘ng qism blok 64 bit;
-:CHap qism blok 16 bit, o‘ng qism blok 16 bit;
I:
S: 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta?
+: 18 ta;
-:19 ta
-:11 ta
-:9 ta
I:
S: 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta?
+: 3 ta
-:7 ta
-:8 ta;
-:9 ta
I:
S: Qaysi formula qoldiqli bo’lish qonunini ifodalaydi
+: a = $bq + r$, $0 \leq r \leq b$,
-:$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$
-:M=r1^k2;
-:M=$\sqrt{k1 + k2}$
I:
S: Eyler funksiyasida p=11 va q=13 sonining qiymatini toping.
+: 16
-:59
-:30
-:21
I:
S: Eyler funksiyasi yordamida 1811 sonining qiymatini toping.

+: 1810
-:2111
-:16
-:524
I:
S: 97 tub sonmi?
+: Tub
-:murakkab
-:Natural
-:To’g’ri javob yo’q
I:
S: Quyidagi modulli ifodani qiymatini toping
(148 + 14432) mod 256.
+: 244
-:200
-:156
-:154
I:
S: Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220
+: 44
-:21
-:42
-:20
I:
S: Quyidagi ifodani qiymatini toping. -16mod11
+: 6
-:5
-:7
-:11
I:
S: 2 soniga 10 modul bo’yicha teskari sonni toping.
+: Ø
-:3
-:10
-:25
I:
S: 2 soniga 10 modul bo’yicha teskari sonni toping.
+: Ø
-:3
-:10
-:25
I:
S: DES da dastlabki kalit uzunligi necha bitga teng?
+:56 bit
-:128 bit
-:64 bit
-:32 bit
I:

1861. S: DES da bloklar har birining uzunligi necha bitga teng?
1862. +:32 bit
1863. -:56 bit
1864. -:48 bit
1865. -:64 bit
1866. I:
1867. S: DES da raundlar soni nechta?
1868. +:16
1869. -:32
1870. -:8
1871. -:48
1872. I:
1873. S: Shifrlash kaliti noma’lum bo’lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi
1874. +:kriptobardoshlik
1875. -:Shifr matn uzunligi
1876. -:Shifrlash algoritmi
1877. -:Texnika va texnologiyalar
1878. I:
1879. S: Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo’linadi
1880. +:blokli va oqimli
1881. -:DES va oqimli
1882. -:Feystel va Verman
1883. -:SP– tarmoq va IP
1884. I:
1885. S: DES shifrlash algoritmida shifrlanadigan malumotlar bloki necha bit?
1886. +:64
1887. -:32
1888. -:48
1889. -:56
1890. I:
1891. S: XOR amali qanday amal?
1892. +:2 modul bo`yicha qo`shish
1893. -:2^{64} modul bo`yicha qo`shish
1894. -:2^{32} modul bo`yicha qo`shish
1895. -:2^{48} modul bo`yicha qo`shish
1896. I:
1897. S: 4+31 mod 32 ?
1898. +:3
1899. -:4
1900. -:31
1901. -:32
1902. I:
1903. S: 21+20mod32?
1904. +:9
1905. -:12
1906. -:16

1907. -:41
1908. I:
1909. S: 12+22 mod 32 ?
1910. +:2
1911. -:12
1912. -:22
1913. -:32
1914. I:
1915. S: AES algoritmi bloki uzunligi … bitdan kam bo'lmasligi kerak.
1916. +:128
1917. -:512
1918. -:256
1919. -:192
1920. I:
1921. S: Xesh-:funktsiyani natijasi …
1922. +:fiksirlangan uzunlikdagi xabar
1923. -:Kiruvchi xabar uzunligidagi xabar
1924. -:Kiruvchi xabar uzunligidan uzun xabar
1925. -:fiksirlanmagan uzunlikdagi xabar
1926. I:
1927. S: 2+5 mod32 ?
1928. +:7
1929. -:32
1930. -:2
1931. -:5
1932. I:
1933. S: 97 tub sonmi?
1934. +:Tub
1935. -:murakkab
1936. -:Natural
1937. -:To'g'ri javob yo'q
1938. I:
1939. S: Ikkilik sanoq tizimida berilgan 10111 sonini o'nlik sanoq tizimiga o'tkazing.
1940. +:23
1941. -:20
1942. -:21
1943. -:19
1944. I:
1945. S: Quyidagi ifodani qiymatini toping. -17mod11
1946. +:5
1947. -:6
1948. -:7
1949. -:11
1950. I:
1951. S: Diskni shifrlash nima uchun amalga oshiriladi?
1952. +: Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidensialligini ta'minlash uchun amalga oshiriladi

-:Xabarni yashirish uchun amalga oshiriladi
-:Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi
-:Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi
I:
S: Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?
+: 4
-:8
-:7
-:5
I:
S: OSI modelida nechta tarmoq satxi bor
+: 7
-:6
-:5
-:4
I:
S: Diskni shifrlash nima uchun amalga oshiriladi?
+: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
-:Xabarni yashirish uchun amalga oshiriladi
-:Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi
-:Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi
I:
S: Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?
+: 4
-:8
-:7
-:5
I:
S: OSI modelida nechta tarmoq satxi bor
+: 7
-:6
-:5
-:4
I:
S: “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonun moddadan iborat
+:16
-:18
-:11
-:14
I:
S: Kompyuter etikasi instituti notijoriy tashkilot tomonidan texnologiyani axloqiy nuqta nazardan targ‘ib qilish bo‘yicha nechta etika qoidalari keltirilgan

1994. +:10
1995. -:18
1996. -:11
1997. -:14
1998. I:
1999. S: Kiberjinoyatchilik bu –. . .
2000. +: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.
2001. -: Kompyuter o‘yinlari
2002. -: Faqat banklardan pul o‘g‘irlanishi
2003. -: autentifikatsiya jarayonini buzish
2004. I:
2005. S: Fishing nima?
2006. +: Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.
2007. -: Ma’lumotlar bazalarini xatoligi
2008. -: Mualliflik huquqini buzilishi
2009. -: Lug‘at orqali xujum qilish.
2010. I:
2011. S: Bag nima?
2012. +: Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo
2013. -: Mualliflik huquqini buzilishi
2014. -: Dasturlardagi ortiqcha reklamalar
2015. -: Autentifikatsiya jarayonini buzish
2016. I:
2017. S: Nuqson nima?
2018. +: Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi nuqsondir
2019. -: Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo
2020. -: Dasturlardagi ortiqcha reklamalar
2021. -: Autentifikatsiya jarayonini buzish
2022. I:
2023. S: Quyidagilardan qaysi birida xavfsiz dasturlash tillari keltirilgan.
2024. +: C#, Scala, Java
2025. -: C, C#, java
2026. -: C++, Scala, Java
2027. -: Misra-C, Java, c++
2028. I:
2029. S: Quyidagilardan qaysi biri dasturiy maxsulotlarga qo‘yiladigan xavfsizlik talablari hisoblanidi.
2030. +: Vazifaviy, novazifaviy, qolgan talablar
2031. -: Qolgan talablar, anaviy taablar, etika talablari
2032. -: Vazifaviy, novazifaviy, etika talablari.
2033. -: Vazifaviy, etika talablari, foydalanuvchanlik talablari.
2034. I:

2035. S: Dasturiy ta’minotda kirish va chiqishga aloqador bo‘lgan talablar qanday talablar sirasiga kiradi?
2036. +:Vazifaviy
2037. -: Novazifaviy
2038. -: Etika talablari
2039. -: Qolgan talablar
2040. I:
2041. S: Dasturda tizim amalga oshirishi kerak bo‘lgan vazifalar bu..
2042. +:Vazifaviy
2043. -: Novazifaviy
2044. -: Etika talablari
2045. -: Qolgan talablar
2046. I:
2047. S: Risklarni boshqarishda risklarni aniqlash jarayoni bu-..
2048. +: Tashkilot xavfsizligiga ta’sir qiluvchi tashqi va ichki risklarning manbasi, sababi, oqibati va haklarni aniqlash.
2049. -: Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta’siri va ehtimolini o‘lchashni ta’minlaydi.
2050. -: Risklarni davolash bu – aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni.
2051. -: Risk monitoringi yangi risklarni paydo bo‘lish imkoniyatini aniqlash.
2052. I:
2053. S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.
2054. +:"Sovuq saxiralash"
2055. -:"Issiq zaxiralash"
2056. -:"Iliq saxiralash"
2057. -:"To'liq zaxiralash"
2058. I:
2059. S: Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishi bilan bog'liq bo'lsa bu nima deb yuritiladi?
2060. +:Jinoyat sifatida baholanadi
2061. -:Rag’bat hisoblanadi
2062. -:Buzgunchilik hisoblanadi
2063. -:Guruhlar kurashi hisoblanadi
2064. I:
2065. S: Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun qanday kalit ishlatiladi?
2066. +:Ikkita kalit
2067. -:Bitta kalit
2068. -:Elektron raqamli imzo
2069. -:Foydalanuvchi identifikatori
2070. I:
2071. S:Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?
2072. +:Axborot xavfsizligi buzulgan taqdirda ko’rilishi mumkin bo’lgan zarar miqdori bilan
2073. -:Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhumligi bilan

2074. -:Axborotni noqonuniy foydalanishlardan o’zgartirishlardan va yo’q qilishlardan himoyalanganligi bilan
2075. -:Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bilan}
2076. I:
2077. S:Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?
2078. +:Strukturalarni ruxsatsiz modifikatsiyalash
2079. -:Tabiy ofat va avariya
2080. -:Texnik vositalarning buzilishi va ishlamasligi
2081. -:Foydalanuvchilar va xizmat ko‘rsatuvchi hodimlarning hatoliklari}
2082. I:
2083. S:Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?
2084. +:Texnik vositalarning buzilishi va ishlamasligi
2085. -:Axborotdan ruhsatsiz foydalanish
2086. -:Zararkunanda dasturlar
2087. -:An’anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili}
2088. I:
2089. S:Axborot xavfsizligini ta'minlovchi choralarni ko’rsating?
2090. +:1-huquqiy, 2-tashkiliy-ma'muriy, 3-injener-texnik
2091. -:1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy
2092. -:1-dasturiy, 2-tashkiliy-ma'muriy, 3-huquqiy
2093. -:1-aparat, 2-texnikaviy, 3-huquqiy}
2094. I:
2095. S:Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o’z ichiga oladi
2096. +:Xalqaro va milliy huquqiy me’yorlarni
2097. -:Tashkiliy va xalqaro me’yorlarni
2098. -:Ananaviy va korporativ me’yorlarni
2099. -:Davlat va nodavlat tashkilotlarime’yorlarni}
2100. I:
2101. S:Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?
2102. +: Ma’lumotlar butunligi
2103. -:Axborotning konfedensialligi
2104. -:Foydalanuvchanligi
2105. -:Ixchamligi}

2106. I:
2107. S:Axborotning buzilishi yoki yo‘qotilishi xavfiga olib keluvchi himoyalanuvchi ob’ektga qarshi qilingan xarakatlar qanday nomlanadi?
2108. +:Tahdid
2109. -:Zaiflik
2110. -:Hujum
2111. -:Butunlik}
2112. I:
2113. S:Biometrik autentifikatsiyalashning avfzalliklari-bu:

2114. +:Biometrik alomatlarning noyobligi
2115. -:Bir marta ishlatilishi
2116. -:Biometrik alomatlarni o’zgartirish imkoniyati
2117. -:Autentifikatsiyalash jarayonining soddaligi
2118. I:
2119. S: Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari-bu:
2120. +:Foydalanuvchanligi
2121. -:Ma’lumotlar butunligi
2122. -:Axborotning konfedensialligi
2123. -:Ixchamligi
2124. I:
2125. S:Global simsiz tarmoqning ta`sir doirasi qanday?
2126. +:Butun dunyo bo’yicha
2127. -:Binolar va korpuslar
2128. -:O’rtacha kattalikdagishahar
2129. -:Foydalanuvchi yaqinidagi tarmoq
2130. I:
2131. S: Foydalanuvchini identifikatsiyalashda qanday ma’lumotdan foydalaniladi?
2132. +:Identifikatori
2133. -:Telefon raqami
2134. -:Parol
2135. -:Avtorizatsiyasi
2136. I:
2137. S: Foydalanuvchining tarmoqdagi harakatlarini va resurslardan foydalanishga urinishini qayd etish-bu:
2138. +:Ma`murlash
2139. -:Autentifikatsiya
2140. -:Identifikatsiya
2141. -:Sertifikatsiyalash
2142. I:
2143. S: Kompyuter tizimini ruxsatsiz foydalanishdan himoyalashni, muhim kompyuter tizimlarni rezervlash, o‘g‘irlash va diversiyadan himoyalanishni ta’minlash rezerv elektr manbai, xavfsizlikning maxsus dasturiy va apparat vositalarini ishlab chiqish va amalga oshirish qaysi choralarga kiradi?
2144. +:Injener-texnik
2145. -:Molyaviy
2146. -:Tashkiliy-ma’muriy
2147. -:Huquqiy
2148. I:
2149. S: Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi-bu:
2150. +:Autentifikatsiya
2151. -:Identifikatsiya
2152. -:Ma`murlash (accaunting)
2153. -:Avtorizatsiya
2154. I:

2155. S: O‘zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi–bu:
2156. +:Tarmoq viruslari
2157. -:Pochta viruslari
2158. -:Fayl viruslari
2159. -:Protokol viruslari
2160. I:
2161. S: Qanday viruslar xavfli hisoblanadi?
2162. +:kompyuter ishlashida jiddiy nuqsonlarga olib keluvchi
2163. -:Jiddiy nuqsonlarga olib kelmaydigan ammo foydalanuvchini chalg'itadigan.
2164. -:Katta viruslar va odatda zararli dasturlar
2165. -:Passiv viruslar
2166. I:
2167. S: Rezident bo’lmagan viruslar qachon xotirani zararlaydi?
2168. +:Faqat faollashgan vaqtida
2169. -:Faqat o’chirilganda
2170. -:Kompyuter yoqilganda
2171. -:Tarmoq orqali ma’lumot almashishda
2172. I:
2173. S: Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan iborat?
2174. +:Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud
2175. -:Tarmoq chetki nuqtalari orasidagi xududning kengligi asosida qurilmalarholati
2176. -:Himoya vositalarining chegaralanganligi
2177. -:Himoyani amalga oshirish imkoniyati yo‘qligi va ma'lum protokollarning ishlatilishi
2178. I:
2179. S: Simmetrik shifrlashning noqulayligi – bu:
2180. +:Maxfiy kalitlar bilan ayirboshlash zaruriyatidir
2181. -:Kalitlar maxfiyligi
2182. -:Kalitlar uzunligi
2183. -:SHifrlashga ko‘p vaqt sarflanishi va ko'p yuklanishi
2184. I:
2185. S: Simsiz tarmoqlarni kategoriyalarini to’g’ri ko’rsating?
2186. +:Simsiz shaxsiy tarmoq (PAN), simsiz lokal tarmoq (LAN), simsiz regional tarmoq (MAN) va Simsiz global tarmoq (WAN)
2187. -:Simsiz internet tarmoq (IAN)va Simsiz telefon tarmoq (WLAN), Simsiz shaxsiy tarmoq (PAN) va Simsiz global tarmoq (WIMAX)
2188. -:Simsiz internet tarmoq (IAN) va uy simsiz tarmog’i
2189. -:Simsiz chegaralanmagan tarmoq (LAN), simsiz kirish nuqtalari

2190. I:
2191. S: Sub`ektga ma`lum vakolat va resurslarni berish muolajasi-bu:
2192. +:Avtorizatsiya
2193. -:Haqiqiylikni tasdiqlash
2194. -:Autentifikatsiya
2195. -:Identifikasiya

2196. I:
2197. S: Tarmoq operatsion tizimining to'g'ri konfiguratsiyasini madadlash masalasini odatda kim hal etadi?
2198. +:Tizim ma'muri
2199. -:Tizim foydalanuvchisi
2200. -:Korxona raxbari
2201. -:Operator
2202. I:
2203. S: Tarmoqlararo ekran texnologiyasi-bu:
2204. +:Ichki va tashqi tarmoq o’rtasida filtr va himoya vazifasini bajaradi
2205. -:Ichki va tashqi tarmoq o’rtasida axborotni o’zgartirish vazifasini bajaradi
2206. -:Qonuniy foydalanuvchilarni himoyalash
2207. -:Ishonchsiz tarmoqdan kirishni boshqarish}
2208. I:
2209. S: Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko’rsating?
2210. +:DDoS (Distributed Denial of Service) hujum
2211. -:Tarmoq hujumlari
2212. -:Dastur hujumlari asosidagi (Denial of Service) hujum
2213. -:Virus hujumlari}
2214. I:
2215. S: Uyishtirilmagan tahdid, ya’ni tizim yoki dasturdagi qurilmaning jismoniy xatoligi – bu…
2216. +:Tasodifiy tahdid
2217. -:Uyishtirilgan tahdid
2218. -:Faol tahdid
2219. -:Passiv tahdid
2220. I:
2221. S: Axborot xavfsizligi qanday asosiy xarakteristikalarga ega?
2222. +:Butunlik, konfidentsiallik, foydalana olishlik
2223. -:Butunlik, himoya, ishonchlilikni urganib chiqishlilik
2224. -:Konfidentsiallik, foydalana olishlik
2225. -:Himoyalanganlik, ishonchlilik, butunlik
2226. }
2227. I:
2228. S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.
2229. +:"Sovuq saxiralash"
2230. -:"Issiq zaxiralash"
2231. -:"Iliq saxiralash"
2232. -:"To'liq zaxiralash"
2233. I:
2234. S: Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?
2235. +:"Issiq zaxiralash"
2236. -:"Sovuq saxiralash"
2237. -:"Iliq saxiralash"
2238. -:"To'liq zaxiralash"

2239. I:
2240. S: Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang
2241. +:HandyBakcup
2242. -:Recuva, R.saver
2243. -:Cryptool
2244. -:Eset32
2245. I:
2246. S: O'chirilgan, formatlangan ma'lumotlarni tikovchi dasturni belgilang.
2247. +:Recuva, R.saver
2248. -:HandyBakcup
2249. -:Cryptool
2250. -:Eset32
2251. I:
2252. S: Virtuallashtirishga qaratilgan dasturiy vositalarni belgilang.
2253. +:VMware, VirtualBox
2254. -:HandyBakcup
2255. -:Eset32
2256. -:Cryptool
2257. I:
2258. S: Cloud Computing texnologiyasi nechta katta turga ajratiladi?
2259. +:3 turga
2260. -:2 turga
2261. -:4 turga
2262. -:5 turga
2263. I:
2264. S: O'rnatilgan tizimlar-bu…
2265. +:Bu ko'pincha real vaqt hisoblash cheklovlariga ega bo'lgan kattaroq mexanik yoki elektr tizimidagi maxsus funksiyaga ega, boshqaruvchidir
2266. -:Korxona ichki tarmog’iga ulangan korporativ tarmog’idan bo'ladigan hujumlardan himoyalash
2267. -:Korxona ichki tarmog’ini Internet global tarmog’idan ajratib qo’yish
2268. -:Bu ko'pincha global tizimda hisoblash cheklovlariga ega bo'lgan mexanik yoki elektr tizimidagi maxsus funksiyaga ega qurilmadir
2269. I:
2270. S: Axborotdan oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan?
2271. +:AQSH sog'liqni saqlash va insonlarga xizmat ko'rsatish vazirligi
2272. -:AQSH Mudofaa vazirligi
2273. -:O'zbekiston Axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi
2274. -:Rossiya kiberjinoyatlarga qarshu kurashish davlat qo'mitasi
2275. I:
2276. S: Axborotdan oqilona foydalanish kodeksi nechanchi yil ishlab chiqilgan?
2277. +:1973 yil
2278. -:1980 yil
2279. -:1991 yil
2280. -:2002 yil
2281. I:

2282. S: Kompyuter bilan bog'liq falsafiy soha bo'lib, foydalanuvchilarning xatti-harakatlari, komyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko'rsatishini o'rgatadigan soha nima deb ataladi?
2283. +:Kiberetika
2284. -:Kiberhuquq
2285. -:Kiberqoida
2286. -:Kiberxavfsizlik
2287. I:
2288. S: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…
2289. +:Kiberjinoyat
2290. -:Kibersport
2291. -:Kiberterror
2292. -:Hakerlar uyushmasi
2293. I:
2294. S: Tarmoqlararo ekran paket filtrlari qaysi sathda ishlaydi?
2295. +:Tarmoq sathida
2296. -:Ilova sathida
2297. -:Kanal sathida
2298. -:Fizik sathida
2299. I:
2300. S: Tarmoqlararo ekran ekspert paketi filtrlari qaysi sathda ishlaydi?
2301. +:Transport sathida
2302. -:Ilova sathida
2303. -:Kanal sathida
2304. -:Fizik sathida
2305. I:
2306. S: Spam bilan kurashishning dasturiy uslubida nimalar ko’zda tutiladi?
2307. +:Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida filtrlanib cheklanadi
2308. -:Elektron pochta qutisiga kelib tushadigan spamlar me’yoriy xujjatlar asosida cheklanadi va bloklanadi
2309. -:Elektron pochta qutisiga kelib tushadigan spamlar ommaviy ravishda cheklanadi
2310. -:Elektron pochta qutisiga kelib spamlar mintaqaviy hududlarda cheklanadi
2311. I:
2312. S: Ma’lumotlarni yo’qolish sabab bo’luvchi tabiiy tahdidlarni ko’rsating
2313. +:Zilzila, yong‘in, suv toshqini va hak
2314. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
2315. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
2316. -:Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani
2317. I:
2318. S: Ma’lumotlarni tasodifiy sabablar tufayli yo’qolish sababini belgilang
2319. +:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

2320. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
2321. -:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
2322. -:Zilzila, yong‘in, suv toshqini va hak
2323. I:
2324. S: Ma’lumotlarni inson xatosi tufayli yo’qolish sababini belgilang.
2325. +:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
2326. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
2327. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
2328. -:Zilzila, yong‘in, suv toshqini va hak
2329. I:
2330. S: Ma’lumotlarni g’arazli hatti harakatlar yo’qolish sababini ko’rsating.
2331. +:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
2332. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
2333. -:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
2334. -:Zilzila, yong‘in, suv toshqini va hak
2335. I:
2336. S: Kompyuterda hodisalar haqidagi ma’lumot qayerda saqlanadi?
2337. +:Hodisalar jurnaliga
2338. -:Operativ xotiraga
2339. -:Kesh xotiraga
2340. -:Vaqtinchalik faylga
2341. I:
2342. S: Internet orqali masofada joylashgan kompyuterga yoki tarmoq resurslariga DoS hujumlari uyushtirilishi natijasida..
2343. +:Foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan mahrum qilinadilar
2344. -:Foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzg’unchilarga etkaziladi
2345. -:Axborot tizimidagi ma’lumotlar bazalari o’g’irlanib ko’lga kiritilgach, ular yo’q qilinadilar
2346. -:Foydalanuvchilar axborotlariga ruxsatsiz o’zgartirishlar kiritilib, ularning yaxlitligi buziladi
2347. I:
2348. S: Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo’naltirilgan buzg’unchi bu - ... .
2349. +:Krakker
2350. -:Hakker
2351. -:Virus bot
2352. -:Ishonchsiz dasturchi
2353. I:

2354. S: Antivirus dasturiy vositalari viruslarni tahlil qilishiga ko'ra necha turga bo'linadi?
2355. +:2 turga: fayl Signaturaga va evristikaga asoslangan
2356. -:2 turga: faol va passiv
2357. -:2 turga: pulli va pulsiz
2358. -:2 turga: litsenziyali va ochiq
2359. I:
2360. S: "Parol', "PIN"' kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?
2361. +:Foydalanish davrida maxfiylik kamayib boradi
2362. -:Parolni esda saqlash kerak bo'ladi
2363. -:Parolni almashtirish jarayoni murakkabligi
2364. -:Parol uzunligi soni cheklangan
2365. I:
2366. S: Yaxlitlikni buzilishi bu - …
2367. +:Soxtalashtirish va o’zgartirish
2368. -:Ishonchsizlik va soxtalashtirish
2369. -:Soxtalashtirish
2370. -:Butunmaslik va yaxlitlanmaganlik
2371. I:
2372. S: Tarmoqda joylashgan fayllar va boshqa resurslardan foydalanishni taqdim etuvchi tarmoqdagi kompyuter nima?
2373. +:Server
2374. -:Bulutli tizim
2375. -:Superkompyuter
2376. -:Tarmoq
2377. I:
2378. S: Tahdid nima?
2379. +:Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.
2380. -:Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa
2381. -:Bu riskni o‘zgartiradigan harakatlar bo‘lib
2382. -:Bu noaniqlikning maqsadlarga ta’siri
2383. I:
2384. S: Risk nima?
2385. +:Potensial kuchlanish yoki zarar
2386. -:Potensial foyda yoki zarar
2387. -:Tasodifiy taxdid
2388. -:Katta yo‘qotish
2389. I:
2390. S: Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi?
2391. +:Optik tolali
2392. -:O’rama juft
2393. -:Koaksial
2394. -:Telefon kabeli
2395. I:
2396. S: Nima uchun autentifikatsiyalashda parol ko’p qo’llaniladi?
2397. +:Sarf xarajati kam, almashtirish oson
2398. -:Parolni eslab qolish oson

-:Parolni o’g’rishlash qiyin
-:Serverda parollarni saqlash oson
I:
S: Elektron xujjatlarni yo’q qilish usullari qaysilar?
+:Shredirlash, magnitsizlantirish, yanchish
-:Yoqish, ko’mish, yanchish
-:Shredirlash, yoqish, ko’mish
-:Kimyoviy usul, yoqish.
I:
S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?
+:Imzo qo‘yish va imzoni tekshirishdan
-:Faqat imzo qo‘yishdan
-:Faqat imzoni tekshirishdan
-:Kalitlarni taqsimlashdan
I:
S: Elektron pochtaga kirishda foydalanuvchi qanday autetntifikasiyalashdan o’tadi?
+:Parol asosida
-:Smart karta asosida
-:Biometrik asosida
-:Ikki tomonlama
I:
S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Jazolar bosqichiga to‘g‘ri ta’rif berilgan.
-: tashkilot o‘z siyosatini ishlab chiqishdan oldin o‘z aktivlari uchun risklarni baholashi shart
-: tashkilot o‘z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o‘rnatilish shart
-: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo‘shimcha kiritish jarayonida boshqaruvchi bo‘lishi shart
+: ma’lum tashkilotlarda tashkilotlarda qat’iy siyosatlar mavjud. Agar xodimlar ushbu siyosatlarga amal qilmasa, ularga qarshi bir qancha choralar qo‘llaniladi.
I:
S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Xodimlarni o‘rgatish bosqichiga to‘g‘ri ta’rif berilgan.
-: tashkilot o‘z siyosatini ishlab chiqishdan oldin o‘z aktivlari uchun risklarni baholashi shart
-: tashkilot o‘z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o‘rnatilish shart
-: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo‘shimcha kiritish jarayonida boshqaruvchi bo‘lishi shart
+: xodimlarga tashkilot xavfsizlik siyosati davomli ravishda o‘rgatilishi shart
I:
S: Galstuk babochka usuli nima?
+: Risklarni baholash usuli
-: Risklarni qabul qilish usuli

-: shifrlash algoritmi
-: Risklarni hosil qilish usuli.
I:
S: Lotin alifbosida DADA so‘zini 3 kalit bilan shifrlagandan so‘ng qaysi so‘z hosil bo‘ladi. A=0, B=1….Z=25.
+:GDGD
-: NANA
-: GPGP
-: FDFD
I:
S: Lotin alifbosida NON so‘zini 3 kalit bilan shifrlagandan so‘ng qaysi so‘z hosil bo‘ladi. A=0, B=1….Z=25.
-:GDGD
-: NANA
+: QRQ
-: FDFD
I:
S: Fizik to‘siqlarni o‘rnatish , Xavfsizlik qo‘riqchilarini ishga olish, Fizik qulflar qo‘yishni amalga oshirish qanday nazorat turiga kiradi?
+:Fizik nazorat
-: Texnik nazorat
-: Ma’muriy nazorat
-: Tashkiliy nazorat
I:
S: Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?
-: Fizik nazorat
+:Texnik nazorat
-: Ma’muriy nazorat
-: Tashkiliy nazorat
I:
S: Qoida va muolajalarni yaratish, Joylashuv arxitekturasini loyihalash, Xavfsizlik belgilari va ogohlantirish signallari, Ishchi joy xavfsizligini ta’minlash, Shaxs xavfsizligini ta’minlash amalga oshirish qanday nazorat turiga kiradi?
-: Fizik nazorat
-: Texnik nazorat
+: Ma’muriy nazorat
-: Tashkiliy nazorat
I:
S: Ikkilik sanoq tizimida qanday raqamlardan foydalanamiz?
+: Faqat 0 va 1
-: Faqat 1
-: Faqat 0
-: Barcha raqamlardan
I:
S: AES shifrlash algoritmi necha rounddan iborat

2475. +: 10, 12, 14
2476. -: 10,14,16
2477. -: 12,14,16
2478. -: 16
2479. I:
2480. S: Hodisalar daraxti usuli nima?
2481. +: Risklarni baholash usuli
2482. -: Risklarni qabul qilish usuli
2483. -: shifrlash algoritmi
2484. -: Risklarni hosil qilish usuli
2485. I:
2486. S: Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?
2487. +:3 taga
2488. -:4 taga
2489. -:2 taga
2490. -:5 taga

2491. I:
2492. S: WiMAX qanday simsiz tarmoq turiga kiradi.
2493. +: Regional
2494. -: Lokal
2495. -: Global
2496. -: Shaxsiy
2497. I:
2498. S: Wi-Fi necha Gs chastotali to'lqinda ishlaydi?
2499. +: 2.4-5 Gs
2500. -: 2.4-2.485 Gs
2501. -: 1.5-11 Gs
2502. -: 2.3-13.6 Gs
2503. I:
2504. S: Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi?
2505. +: Onx458&hdsh)
2506. +: 12456578
2507. +: salomDunyo
2508. +: Mashina777
2509. I:
2510. S: Parollash siyosatiga ko'ra parol tanlash shartlari qanday?
2511. +: Kamida 8 belgi: katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. -: Kamida 8 belgi: katta va kichik xavflar, sonlar qo'llanishi kerak.
2512. -: Kamida 6 belgi: katta xarflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak.
2513. -: Kamida 6 belgi: katta va kichik xarflar, kamida bitta maxsus simvol qo'llanishi kerak.

1. Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

Foydalanishni boshqarish

2. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?
Xalqa

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

5. Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?
Texnik nazorat

6. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating
Zilzila, yong‘in, suv toshqini va hak.

7. Token, Smartkartalarda xavfsizlik tomonidan kamchiligi nimada?
Qurilmalarni ishlab chiqarish murakkab jarayon

8. Foydalanishni boshqarish –bu...
Sub’ektni Sub’ektga ishlash qobilyatini aniqlashdir.

9. Ro‘yxatdan o‘tish-bu…
foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni

10. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?
Xavfsizlik siyosati ma’muri

11. MD5, SHA1, SHA256, O‘z DSt 1106:2009- qanday algoritmlar deb ataladi?
Shifrlash

12. Shifr nima?
Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm

13. Ethernet kontsentratori qanday vazifani bajaradi?
kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo‘naltirib beradi

14. Tekstni boshqa tekst ichida ma’nosini yashirib keltirish nima deb ataladi?
steganografiya

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

16. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?
1-2 jahon urushu davri

17. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?
Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

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

19. Kriptografiyaning asosiy maqsadi nima?
maxfiylik, yaxlitlilikni ta’minlash

20. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.
ABAC

1. Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?
Foydalanishni boshqarish

2. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?
Xalqa

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

5. Ruxsatlarni nazoratlash, “Qopqon”, Yong‘inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?
Texnik nazorat

6. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating
Zilzila, yong‘in, suv toshqini va hak.

9. Ro‘yxatdan o‘tish-bu…
foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni

10. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?
Xavfsizlik siyosati ma’muri

12. Shifr nima?
Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm

13. Ethernet kontsentratori qanday vazifani bajaradi?
kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo‘naltirib beradi

14. Tekstni boshqa tekst ichida ma’nosini yashirib keltirish nima deb ataladi?
steganografiya

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

16. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?
1-2 jahon urushu davri

17. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?
Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

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

19. Kriptografiyaning asosiy maqsadi nima?
maxfiylik, yaxlitlilikni ta’minlash

1. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.
HandyBakcup

2. Makroviruslar nimalarni zararlaydi?
Ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.

3. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….
Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

4. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?
Ruxsat berishga asoslangan siyosat

5. Nuqson atamasiga berilgan ma’noni ko‘rsating.
Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi

6. Hamma narsa ta’qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?
Paranoid siyosati (Paranoid Policy)

7. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuni qachon kuchga kirgan?
1997 yil 24 aprel

8. Adware-zararli dastur vazifasi nimadan iborat?
marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.

9. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

Strukturalarni ruxsatsiz modifikatsiyalash

10. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?
Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar

11. Fishing (ing. Fishing – baliq ovlash) bu…
Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

12. Ma’lumotlarni zaxira nusxalash bu – …
Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni.

13. ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.
Risk monitoring

14. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.
Recuva, R.saver

15. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?
Foydalanishni boshqarish

16. Kiberetika tushunchasi:
Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

17. Rootkits-qanday zararli dastur?
ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

18. "Fishing" tushunchasi:
Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

19. Enterprise Information Security Policies, EISP-bu…
Tashkilot axborot xavfsizligi siyosati

20. Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi?
Razvedka hujumlari

1. Hamma narsa ta’qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?
Paranoid siyosati (Paranoid Policy)

2. Spam bilan kurashishning dasturiy uslubida nimalar ko‘zda tutiladi?
Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida filtrlanib cheklanadi.

3. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?
Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan

4. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud?
detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar

5. "Axborotlashtirish to‘g‘risida"gi Qonunning maqsadi nimadan iborat?
Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.

6. Ma’lumotlarni bloklarga bo‘lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?
RAID 0

7. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?
Foydalanishni boshqarish

8. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.
Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

9. Doktorlar, detektorlarga xos bo‘lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang.
Faglar

10. Dastlabki virus nechanchi yilda yaratilgan?
1986

11. Rezident virus…
tezkor xotirada saqlanadi

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

13. Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi?
Razvedka hujumlari

14. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?
Detektorlar

15. Makroviruslar nimalarni zararlaydi?
Ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.

16. Texnik himoya vositalari – bu ...
Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob’ektni himoyalashdir

17. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…
Kiberjinoyat deb ataladi

19. Issue-Specific Security Policies, ISSP-bu…
Muammofa qaratilgan xavfsizlik siyosati

20. Axborot xavfsizligin ta'minlashda birinchi darajadagi me’yoriy hujjat nomini belgilang.

qonunlar

1. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.
ABAC

2. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?
Xavfsizlik siyosati ma’muri

3. Kriptografiyaning asosiy maqsadi nima?
maxfiylik, yaxlitlilikni ta’minlash

4. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?
parol

5. Global simsiz tarmoqda qaysi standartlar ishlaydi?
CDPD, 4G

6. Autentifikatsiya faktorlari nechta?
3 ta

8. Kriptografiyada matn –bu..
alifbo elementlarining tartiblangan to‘plami

9. Stenografiya ma’nosi qanday?
sirli yozuv

11. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?
Texnik vositalarning buzilishi va ishlamasligi

12. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?
Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

13. Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?
Xesh funksiyalar

14. WiMAX qanday simsiz tarmoq turiga kiradi?
Regional

15. Simmetrik shifrlashning noqulayligi – bu:
Maxfiy kalitlar bilan ayirboshlash zaruriyatidir

16. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating
Zilzila, yong‘in, suv toshqini va hak.

17. Ma’lumotlarni tasodifiy sabablar tufayli yo‘qolish sababini belgilang
Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

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

Biometrik autentifikatsiya

1. Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?
3 taga

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

3. Autentifikatsiya faktorlari nechta?
3 ta

4. Axborot xavfsizligining asosiy maqsadlaridan biri-bu…
Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish

5. Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.
Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

6. Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi?
Optik tolali

7. Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?
Xesh funksiyalar

8. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?
1-2 jahon urushu davri

9. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.
ABAC

10. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?
Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

11. Sub’ektga ma’lum vakolat va resurslarni berish muolajasi-bu:
Avtorizatsiya

12. Kriptografiyaning asosiy maqsadi nima?
maxfiylik, yaxlitlilikni ta’minlash

13. Identifikatsiya bu- …
Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni

14. Fire Wall ning vazifasi...
Tarmoqlar orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta’minlaydi

15. Kiberjinoyatchilik bu –. . .
Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.

16. Berilgan ta’riflardan qaysi biri asimmetrik tizimlarga xos?

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

17. Biometrik autentifikatsiyalashning avfzalliklari-bu:
Biometrik parametrlarning noyobligi

18. "Parol', "PIN"' kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?
Foydalanish davrida maxfiylik kamayib boradi

19. Kriptografiyada kalitning vazifasi nima?

1. Spyware-qanday zararli dastur?
Foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.

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

3. Adware-zararli dastur vazifasi nimadan iborat?
marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.

4. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.
HandyBakcup

5. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?
RAID 5

6. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?
Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar

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

8. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?
Paranoid siyosat

9. ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.
Risk monitoring

10. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….
Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

11. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko‘rsating?
DDoS (Distributed Denial of Service) hujum

12. Kiberetika tushunchasi:
Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

13. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.
Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

14. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?
Foydalanishni boshqarish

15. Polimorf viruslar tushunchasi to‘g‘ri ko‘rsating.
Viruslar turli ko‘rinishdagi shifrlangan viruslar bo‘lib, o‘zining ikkilik shaklini nusxadan-nusxaga o‘zgartirib boradi

16. Rezident virus…
tezkor xotirada saqlanadi

17. Hamma narsa ta’qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?
Paranoid siyosati (Paranoid Policy)

1. Kiberetika tushunchasi:
Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

2. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?
Foydalanishni boshqarish

3. Doktorlar, detektorlarga xos bo‘lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang.
Faglar

4. Zararli dasturlar qanday turlarga bo‘linadi?
Dasturdagi zaifliklar(atayin qilingan) va zararli dasturlar(atayin qilingan)

5. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu...
Tamoqlararo ekranlarning o‘rnatilishi

6. Bag atamasini nima ma'noni beradi?
Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo

7. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima deyiladi?
Xavfsizlik siyosat

8. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.
HandyBakcup

9. DIR viruslari nimani zararlaydi?
FAT tarkibini zararlaydi

10. ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.
Risk monitoring

11. Nuqson atamasiga berilgan ma’noni ko‘rsating.
Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi

12. “Axborot olish kafolatlari va erkinligi to‘g‘risida”gi Qonunning 10-moddasi mazmuni qanday?

Axborot manbaini oshkor etmaslik

13. Qaysi siyosat turli hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi?
Maqbul foydalanish siyosati

14. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?
Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar

15. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.
Recuva, R.saver

16. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi?
RAID 3

17. Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to‘liq tasavvurga ega shaxs kim deb ataladi?
Xavfsizlik ma'muri (admin)

19. Ma’lumotlarni bloklarga bo‘lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?
RAID 0

20. Qaysi siyosatda Adminstrator xavfsiz va zarur xizmatlarga indvidual ravishda ruxsat beradi?
Extiyotkorlik siyosati

1. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating
Zilzila, yong‘in, suv toshqini va hak.

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

3. Berilgan ta’riflardan qaysi biri asimmetrik tizimlarga xos?
Asimmetrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi

6. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?
1-2 jahon urushu davri

7. Wi-Fi necha Gs chastotali to‘lqinda ishlaydi?
2.4-5 Gs

8. Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi.
WEP, WPA, WPA2

11. Konfidentsiallikga to‘g‘ri ta’rif keltiring.
axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

12. Autentifikatsiya nima?

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

13. Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?
Ma’lumotlar butunligi

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

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

16. Kodlash nima?
Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

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

18. Kriptografiyada kalitning vazifasi nima?
Matnni shifrlash va shifrini ochish uchun kerakli axborot

19. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?
Xalqa

20. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?
Texnik vositalarning buzilishi va ishlamasligi

1. Konfidentsiallikga to‘g‘ri ta’rif keltiring.
axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

2. Foydalanishni boshqarish –bu...
Sub’ektni Ob’ektga ishlash qobilyatini aniqlashdir.

3. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so‘z) – nima?
parol

4. To‘rtta bir-biri bilan bog‘langan bog‘lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?
Xalqa

5. Kodlash nima?
Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

6. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?
Yulduz

7. Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?
Ma’lumotlar butunligi

8. Wi-Fi necha Gs chastotali to‘lqinda ishlaydi?
2.4-5 Gs

9. Yaxlitlikni buzilishi bu - …
Soxtalashtirish va o‘zgartirish

10. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?
1-2 jahon urushu davri

11. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?
Strukturalarni ruxsatsiz modifikatsiyalash

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

13. Risk nima?
Potensial foyda yoki zarar

14. Assimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?
Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun

15. Ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi?
4 xil

16. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?
Xavfsizlik siyosati ma’muri

17. Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.
Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.

3. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….
Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

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

5. Rootkits-qanday zararli dastur?
ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

6. Qaysi texnologiyada ma’lumotni ko‘plab nusxalari bir vaqtda bir necha disklarga yoziladi?
RAID 1

7. "Axborotlashtirish to‘g‘risida"gi Qonunning maqsadi nimadan iborat?

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

8. Hamma narsa ta’qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?
Paranoid siyosati (Paranoid Policy)

10. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?
Paranoid siyosat

11. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.
"Sovuq saxiralash"

12. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?
Detektorlar

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

14. "Fishing" tushunchasi:
Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

15. O‘zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunning qaysi moddasi sabab qilib olingan?
27(1)-modda. O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berishning alohida shartlari

16. Ma’lumotlarni zaxira nusxalash bu – …
Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni.

17. Fishing (ing. Fishing – baliq ovlash) bu…
Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

18. Dastlabki virus nechanchi yilda yaratilgan?
1986

19. "Backdoors"-qanday zararli dastur?
zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

20. Kiberetika tushunchasi:
Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

3. Ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi?
4 xil

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

5. Rol tushunchasiga ta’rif bering.
Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin

6. Identifikatsiya bu- …
Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni

7. Shifr nima?
Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm

8. Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.
Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

10. Stenografiya ma’nosi qanday?
sirli yozuv

11. OSI modelida nechta sath mavjud?
7 ta

12. Kriptografiyada kalitning vazifasi nima?
Matnni shifrlash va shifrini ochish uchun kerakli axborot

13. Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi?
Shaxsiy tarmoq

15. Risk nima?
Potensial foyda yoki zarar

16. Kodlash nima?
Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir

17. Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.
ABAC

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

19. Zamonaviy kriptografiya qanday bo‘limlardan iborat?
Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish

1. Spam bilan kurashishning dasturiy uslubida nimalar ko‘zda tutiladi?
Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida filtrlanib cheklanadi.

2. Ma’lumotlarni bloklarga bo‘lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?
RAID 0

3. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.

"Sovuq saxiralash"

4. Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to‘liq tasavvurga ega shaxs kim deb ataladi?
Xavfsizlik ma'muri (admin)

5. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?
RAID 5

6. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima deyiladi?
Xavfsizlik siyosat

7. Fishing (ing. Fishing – baliq ovlash) bu…
Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.

8. Bag atamasini nima ma'noni beradi?
Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo

9. "Backdoors"-qanday zararli dastur?
zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

10. Dastlabki virus nechanchi yilda yaratilgan?
1986

11. Virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?
Detektorlar

12. Risk monitoringi ….. ni paydo bo‘lish imkoniyatini aniqlaydi.
Yangi risklar

13. Ransomware qanday zarar keltiradi?
mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi.

14. O‘zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunning qaysi moddasi sabab qilib olingan?
27(1)-modda. O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berishning alohida shartlari

15. Texnik himoya vositalari – bu ...
Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob’ektni himoyalashdir

17. Enterprise Information Security Policies, EISP-bu…
Tashkilot axborot xavfsizligi siyosati

18. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?
Paranoid siyosat

19. "Fishing" tushunchasi:
Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

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

1. "Fishing" tushunchasi:
Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi

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

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

4. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko‘rsating?
DDoS (Distributed Denial of Service) hujum

5. Nuqson atamasiga berilgan ma’noni ko‘rsating.
Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi

6. Risklarni identifikatsiya qilishdan maqsad nima?
Potensial zarar yetkazadigan ehtimoliy insidentlarni prognozlash va bu zarar qay tarzda olinishi mumkinligi to‘g‘risida tasavvurga ega bo‘lish

7. Dastlabki virus nechanchi yilda yaratilgan?
1986

8. Rootkits-qanday zararli dastur?
ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

9. Qaysi siyosatga ko‘ra hamma narsa ta'qiqlanadi?
Paranoid siyosat

10. Ko‘p platformali viruslar bu…
Bir vaqtning o‘zida turli xildagi ob’ektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlaydi

11. “Axborot olish kafolatlari va erkinligi to‘g‘risida”gi Qonunning 10-moddasi mazmuni qanday?
Axborot manbaini oshkor etmaslik

12. Risk monitoringi ….. ni paydo bo‘lish imkoniyatini aniqlaydi.
Yangi risklar

13. “Elektron hujjat” tushunchasi haqida to‘g‘ri ta’rif berilgan qatorni ko‘rsating.
Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir

15. O‘zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunning qaysi moddasi sabab qilib olingan?
27(1)-modda. O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berishning alohida shartlari

16. Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?
RAID 5

17. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?
Strukturalarni ruxsatsiz modifikatsiyalash

18. "Backdoors"-qanday zararli dastur?
zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish

19. Botnet-nima?
internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi.

20. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?
Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan

Windows OT lokal xavfsizlik siyosatini sozlash oynasiga o'tish uchun "Buyruqlar satri"ga quyidagi so'rovlardan qaysi biri kiritiladi?

J:secpol.msc

OSI modelida nechta tarmoq satxi bor ?

J: 7

OSI modelining birinchi satxi qanday nomlanadi

J: Fizik satx

OSI modelining ikkinchi satxi qanday nomlanadi

J: Kanal satxi

OSI modelining uchinchi satxi qanday nomlanadi

J: Tarmoq satxi

OSI modelining oltinchi satxi qanday nomlanadi

J: Taqdimlash satxi

OSI modelining yettinchi satxi qanday nomlanadi

J: Amaliy satx

OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi

J: fizik, kanal va tarmoq satxlari

OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi

J: Marshrutizator

OSI modelining fizik satxi qanday funktsiyalarni bajaradi

J: Elektr signallarini uzatish va qabul qilish

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

J: Obyekt

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

J: Subyekt

Simmetrik kriptotizimlarda ... jumlani davom ettiring

J: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi

Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.

J: 2 turga

Axborotning eng kichik o’lchov birligi nima?

J: bit

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

J: Biometrik autentifikatsiya

Kriptografiyaning asosiy maqsadi...

J: maxfiylik, yaxlitlilikni ta`minlash

Ro’yxatdan o’tish bu?

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

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

J: Zararli hujumlar

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

J: Kirish hujumlari

Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub

J: Ethernet, FDDI

Xesh-:funktsiyani natijasi …

J: fiksirlangan uzunlikdagi xabar

Ethernet kontsentratori qanday vazifani bajaradi

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

Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?

J: fleshka, CD va DVD disklar

Faol hujum turi deb…

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

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

J: MAC

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

J: DAC

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

J: DAC

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

J: ABAC

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

J: RBAC

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

J: Xalqa Yulduz To’liq bog’lanishli Yacheykali

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

J: DNS tizimlari, Razvedka hujumlari

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

J: Kiberxavfsizlik

Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?

J: raqamli imzoni shakllantirish va tekshirish muolajasi

Kriptologiya -:

J: axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi

Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi?

J: Deshifrlash

Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.

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

Autentifikatsiya faktorlari nechta

J: 3

Kriptografiyada matn –

J: alifbo elementlarining tartiblangan to’plami

Konfidentsiallikga to’g’ri ta`rif keltiring.

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

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

J: login

Kriptoanaliz –

J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

Axborot qanday sifatlarga ega bo’lishi kerak?

J: ishonchli, qimmatli va to’liq

Shifrlash –

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

Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?

J: simmetrik kriptosistemalar

Foydalanishni boshqarish –bu...

J: Subyektni Obyektga ishlash qobilyatini aniqlashdir.

Kompyuterning tashqi interfeysi deganda nima tushuniladi?

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

Kodlash nima?

J: Ma’lumotni osongina qaytarish uchun hammaga

Tarmoq kartasi bu...

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

Elektron raqamli imzo deb –

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

Hab bu...

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

Switch bu...

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

Axborot xavfsizligining asosiy maqsadlaridan biri-: bu…

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

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

J: parol

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

J: SMTP, POP yoki IMAR

Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi?

J: Tez, aniq va maxfiyligiga

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

J: Yozish

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

J: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari

Kalit – bu …

J: Matnni shifrlash va shifrini ochish uchun kerakli axborot

Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi

J: Fizik satx

Blokli shifrlash-:

J: shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish

Kriptobardoshlilik deb …

J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi

J: Xesh funksiyalar

Kriptografiya –

J: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub

J: TCP,UDP

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

J: steganografiya

Yaxlitlikni buzilishi bu -: …

J: Soxtalashtirish va o’zgartirish

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

J: barchasi

Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub

J: Ethernet, FDDI

Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

J: Foydalanishni boshqarish

Tarmoq repiteri bu…

J: Signalni tiklash yoki qaytarish uchun foydalaniladi.

Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

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

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

J: O‘qish

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

J: xavfsizlik siyosati ma’muri

Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?

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

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

J: Tarmoq satxi

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

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

Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi

J: {d, n} – yopiq, {e, n} – ochiq;

Diskni shifrlash nima uchun amalga oshiriladi?

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

Tahdid nima?

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

Risk

J: Potensial foyda yoki zarar

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

J: Fizik satx

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

J: Avtorizatsiya

Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.

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

Kompyuter tarmoqlari bu –

J: Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan

Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?

J: raqamli imzoni shakllantirish va tekshirish muolajasi

Kriptografiyada matn –

J: alifbo elementlarining tartiblangan to’plami

Autentifikatsiya jarayoni qanday jarayon?

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

Rol tushunchasiga ta’rif bering.

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

Avtorizatsiya jarayoni qanday jarayon?

J: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima

J: Parol

Elektron raqamli imzo deb –

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

TCP/IP modelida nechta satx mavjud

J: 4

Kriptoanaliz –

J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi?

J: Simmetrik va assimetrik

Shifrlash nima?

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

Kriptografiyada alifbo –

J: axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam

Kripto tizimga qo’yiladigan umumiy talablardan biri

J:

Simmetrik kriptotizmning uzluksiz tizimida …

J: ochiq matnning har bir harfi va simvoli alohida shifrlanadi

Axborot resursi – bu?

J: axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi

Stenografiya ma’nosi...

J: sirli yozuv

?
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 toígíri 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 ´Soderjimoeª 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¸ bezopasnostiª ining ´V°sokayaª 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 izmeneniyaª 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 mezonlarª ...{
-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 knigaª, 55 ta sinfdan
-´Uygunlashtirilgan mezonlarª, 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