

<b>№</b>	<b>Savolar</b>	<b>Javoblar</b>
<b>1.</b>	Konfidensiallikni ta'minlash bu - ?	<b>ruxsatsiz o'qishdan himoyalash.</b>
<b>2.</b>	Zararli dasturiy vositalarga qarshi foydalaniluvchi dasturiy vosita bu?	<b>Antivirus</b>
<b>3.</b>	Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat bu?	<b>Hujum</b>
<b>4.</b>	Yong'inga qarshi tizimlarni aktiv chora turiga quyidagilardan qaysilari kiradi?	<b>Yong'inni aniqlash va bartaraf etish tizimi</b>
<b>5.</b>	Yong'inga qarshi kurashishning passiv usuliga kiruvchi choralarni to'g'ri ko'rsatilgan javobni toping?	<b>Minimal darajada yonuvchan materiallardan foydalanish, qo'shimcha etaj va xonalar qurish</b>
<b>6.</b>	Yong'inga qarshi kurashishning aktiv usuli to'g'ri ko'rsatilgan javobni toping?	<b>Tutunni aniqlovchilar, alangani aniqlovchilar va issiqlikni aniqlovchilar</b>
<b>7.</b>	Yo'q qilish usullari orasidan ekologik jihatdan ma'qullanmaydigan va maxsus joy talab qiladigan usul qaysi?	<b>Yoqish</b>
<b>8.</b>	Yo'qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon.	<b>Parolga asoslangan autentifikatsiya.</b>
<b>9.</b>	Yaxlitlikni ta'minlash bu - ?	<b>ruxsatsiz yozishdan himoyalash.</b>
<b>10.</b>	Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko'rsating?	<b>Ochiq kalitli shifrlar.</b>
<b>11.</b>	Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga imkon beruvchi himoya vositasi bu?	<b>Tarmoqlararo ekran.</b>
<b>12.</b>	Xizmatdan vos kechishga qaratilgan hujumlar bu?	<b>Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.</b>
<b>13.</b>	Xesh qiymatlarni yana qanday atash mumkin?	<b>dayjest</b>
<b>14.</b>	Xesh funksiyalarda kolliziya hodisasi bu?	<b>Ikki turli matnlarning xesh qiymatlarini bir xil bo'lishi.</b>
<b>15.</b>	Xesh funksiyalar      funksiya.	<b>kalitsiz kriptografik</b>
<b>16.</b>	VPNning texnik yechim arxitekturasiga ko'ra turlari keltirilgan qatorni aniqlang?	<b>Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN; korporativ tarmoqlararo VPN</b>
<b>17.</b>	Virus aniq bo'lganda va xususiyatlari aniq ajratilgan holatda eng katta samaradorlikka ega zararli dasturni aniqlash usulini ko'rsating?	<b>Signaturaga asoslangan usul</b>
<b>18.</b>	Trafik orqali axborotni to'plashga harakat qilish razvedka hujumlarining qaysi turida amalga oshiriladi?	<b>Passiv</b>
<b>19.</b>	Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting?	<b>Doimo xavfsiz saqlab olib yurish zaruriyati.</b>
<b>20.</b>	Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating?	<b>Fizik o'g'irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar</b>
<b>21.</b>	Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu?	<b>Avtorizatsiya</b>
<b>22.</b>	TCP/IP tarmoq modeli nechta sathdan iborat?	<b>4</b>
<b>23.</b>	Tasodifiy tahdidlarni ko'rsating?	<b>Texnik vositalarning buzilishi va ishlamasligi.</b>
<b>24.</b>	Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi.	<b>Tarmoqlararo ekran.</b>
<b>25.</b>	Tarmoq xavfsizligini buzulishi biznes faoliyatga qanday ta'sir qiladi?	<b>Biznes faoliyatning buzilishi, huquqiy javobgarlikka sababchi bo'ladi.</b>
<b>26.</b>	Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan.	<b>Parolga asoslangan autentifikatsiya.</b>
<b>27.</b>	Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?	<b>1 ta</b>
<b>28.</b>	Signatura (antiviruslarga aloqador bo'lgan) bu-?	<b>Fayldan topilgan bitlar qatori.</b>

29.	Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi shifrlar bu -	<b>ochiq kalitli shifrlar.</b>
30.	Shaxsiy simsiz tarmoqlar qo'llanish sohasini belgilang	<b>Tashqi qurilmalar kabellarining o'rnida</b>
31.	RSA algoritmda $p=5$ , $q=13$ , $e=7$ ga teng bo'lsa, shaxsiy kalitni hisoblang?	<b>7</b>
32.	RSA algoritmda ochiq kalit $e=7$ , $N=35$ ga teng bo'lsa, $M=2$ ga teng ochiq matnni shifrlash natijasini ko'rsating?	<b>23</b>
33.	RSA algoritmda ochiq kalit $e=7$ , $N=143$ ga teng bo'lsa, $M=2$ ga teng ochiq matnni shifrlash natijasini ko'rsating?	<b>128</b>
34.	RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?	<b>1</b>
35.	Razvedka hujumlari bu?	<b>Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi.</b>
36.	Rad etishdan himoyalashda ochiq kalitli kriptotizimlarning qaysi xususiyati muhim hisoblanadi.	<b>Ikkita kalitdan foydalanilgani.</b>
37.	Quyidagilarnig qaysi biri tabiiy tahdidlarga misol bo'la oladi?	<b>Toshqinlar, yong'in, zilzila</b>
38.	Quyidagilarnig qaysi biri sun'iy tahdidlarga misol bo'la oladi?	<b>Bosqinchilik, terrorizm, o'g'irlik</b>
39.	Quyidagilardan qaysilari tarmoq topologiyalari hisoblanadi?	<b>Halqa, yulduz, shina, daraxt</b>
40.	Quyidagilardan qaysilari ananaviy tarmoq turi hisoblanadi?	<b>WAN, MAN, LAN</b>
41.	Quyidagilardan qaysi biri to'liq kompyuter topologiyalarini ifodalamaydi.	<b>LAN, GAN, OSI.</b>
42.	Quyidagilardan qaysi biri tarmoq xavfsizligi muammolariga sabab bo'lmaydi?	<b>Routerlardan foydalanmaslik.</b>
43.	Quyidagilardan qaysi biri tabiiy tahdidga misol bo'ladi?	<b>Yong'in, suv toshishi, harorat ortishi.</b>
44.	Quyidagilardan qaysi biri rad etishdan himoyani ta'minlaydi.	<b>Elektron raqamli imzo tizimi.</b>
45.	Quyidagilardan qaysi biri har ikkala tomonning haqiqiylikini tekshirish jarayonini ifodalaydi?	<b>Ikki tomonlama autentifikatsiya.</b>
46.	Quyidagi xususiyatlardan qaysi biri elektron raqamli imzo tomonidan ta'minlanadi?	<b>Axborot butunligini va rad etishdan himoyalash.</b>
47.	Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas.	<b>Bir tomonlama funksiya bo'lmashligi kerak.</b>
48.	Quyidagi qaysi hujum turi razvedka hujumlari turiga kirmaydi?	<b>Ddos</b>
49.	Quyidagi muammolardan qaysi biri simmetrik kriptotizimlarga xos.	<b>Kalitni taqsimlash zaruriyati.</b>
50.	Quyidagi atamalardan qaysi biri faqat simmetrik blokli shifrlarga xos?	<b>Blok uzunligi.</b>
51.	Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?	<b>ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'lmaydi</b>
52.	Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?	<b>chiqishda fiksirlangan uzunlikdagi qiymatni beradi</b>
53.	Qurbon kompyuteridagi ma'lumotni shifrlab, uni deshifrlash uchun to'lovni amalga oshirishni talab qiluvchi zararli dastur bu-?	<b>Ransomware</b>
54.	Qoida, siyosat, qoida va siyosatni mujassamlashtirgan algoritmlar, majburiyatlar va maslahatlar kabi tushunchalar qaysi foydalanishni boshqarish usuliga aloqador.	<b>Attributga asoslangan foydalanishni boshqarish.</b>
55.	Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo'shimcha apparat va dasturiy vositani talab qiladi?	<b>Lentali disklar.</b>
56.	Qaysi xususiyatlar RAID texnologiyasiga xos emas?	<b>Shaxsiy kompyuterda foydalanish mumkin.</b>
57.	Qaysi usul ob'ektlar va sub'ektlarni klassifikatsiyalashga asoslangan?	<b>Mandatli foydalanishni boshqarish.</b>
58.	Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalanadi?	<b>Dasturiy</b>

59.	Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi?	<b>Apparat</b>
60.	Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi.	<b>Tarmoqlararo ekran.</b>
61.	Qaysi ochiq kalitli algoritm katta sonni faktorlash muammosiga asoslanadi?	<b>RSA algoritmi.</b>
62.	Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan?	<b>Ma'muriy nazoratlash.</b>
63.	Qaysi himoya vositasida mavjud paket shifrlangan holda yangi hosil qilingan mantiqiy paket ichiga kiritiladi?	<b>Virtual Private Network.</b>
64.	Qaysi himoya vositasi yetkazilgan axborotning butunligini tekshiradi?	<b>Virtual Private Network.</b>
65.	Qaysi himoya vositasi tomonlarni autentifikatsiyalash imkoniyatini beradi?	<b>Virtual Private Network.</b>
66.	Qaysi himoya vositasi tarmoqda uzatilayotgan axborotni butunligi, maxfiyligi va tomonlar autentifikatsiyasini ta'minlaydi?	<b>Virtual Private Network.</b>
67.	Qaysi himoya vositasi mavjud IP - paketni to'liq shifrlab, unga yangi IP sarlavha beradi?	<b>Virtual Private Network.</b>

68.	Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?	<b>Barcha javoblar to'g'ri</b>
69.	Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?	<b>Barcha javoblar to'g'ri</b>
70.	Qaysi biometrik parametr eng yuqori universallik xususiyatiga ega?	<b>Yuz tasviri.</b>
71.	Qaysi biometrik parametr eng yuqori takrorlanmaslik xususiyatiga ega?	<b>Ko'z qorachig'i.</b>
72.	Qanday tahdidlar passiv hisoblanadi?	<b>Amalga oshishida axborot strukturasi va mazmunida hech narsani o'zgartirmaydigan tahdidlar</b>
73.	Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.	<b>Biometrik autentifikatsiya.</b>
74.	Portlarni va operatsion tizimni skanerlash razvedka hujumlarining qaysi turida amalga oshiriladi?	<b>Aktiv</b>
75.	Parolni "salt" (tuz) kattaligidan foydalanib xeshlashdan (h(password, salt)) asosiy maqsad nima?	<b>Buzg'unchiga ortiqcha hisoblashni talab etuvchi murakkablikni yaratish.</b>
76.	Parolga asoslangan autentifikatsiya usulining asosiy kamchiligini ko'rsating?	<b>Esda saqlash zaruriyati.</b>
77.	Parolga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating?	<b>Parollar lug'atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum.</b>
78.	Parolga "tuz"ni qo'shib xeshlashdan maqsad?	<b>Tahdidchi ishini oshirish.</b>
79.	Paketlarni snifferlash, portlarni skanerlash, ping buyrug'ini yuborish qanday hujum turiga misol bo'ladi?	<b>Razvedka hujumlari</b>
80.	Paketlarni snifferlash, portlarni skanerlash va Ping buyrug'ini yuborish hujumlari qaysi hujumlar toifasiga kiradi?	<b>Razvedka hujumlari.</b>
81.	Paket filterlari turidagi tarmoqlararo ekran vositasi OSI modelining qaysi sathida ishlaydi?	<b>Tarmoq sathida.</b>
82.	Paket filteri turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi?	<b>Tarmoq sathi parametrlari asosida.</b>
83.	OSI tarmoq modeli nechta sathdan iborat?	<b>7</b>
84.	Ochiq tarmoq yordamida himoyalangan tarmoqni qurish imkoniyatiga ega himoya vositasi bu?	<b>Virtual Private Network.</b>
85.	Ochiq matn qismlarini takroriy shifrllovchi algoritmlar bu -	<b>blokli shifrlar</b>
86.	O'zini yaxshi va foydali dasturiy vosita sifatida ko'rsatuvchi zararli dastur turi bu?	<b>Troyan otlari.</b>
87.	O'zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko'rsating?	<b>"UNICON.UZ" DUK</b>
88.	Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi hodisalarning potensial paydo bo'lishi bu?	<b>Tahdid</b>
89.	Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi zararli dastur turi bu?	<b>Adware</b>
90.	Markaziy xab yoki tugun orqali tarmoqni markazlashgan holda boshqarish qaysi tarmoq topologiyasida amalga oshiriladi?	<b>Yulduz</b>
91.	Ma'lumotni zaxira nusxalash nima uchun potensial tahdidlarni paydo bo'lish ehtimolini oshiradi.	<b>Tahdidchi uchun nishon ko'payadi.</b>
92.	Ma'lumotni to'liq qayta tiklash qachon samarali amalga oshiriladi?	<b>Saqlagichda ma'lumot qayta yozilmagan bo'lsa.</b>
93.	Ma'lumotni shifrlash va deshifrlashda yagona kalitdan foydalanuvchi tizim bu -	<b>simmetrik kriptotizim.</b>
94.	Ma'lumotni mavjudligini yashirishda .....	<b>steganografik algoritmdan</b>

		<b>foydalaniladi.</b>
95.	Ma'lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi?	<b>Zarur axborotni tanlashdan.</b>
96.	Ma'lumot shifrlansa, natijasi bo'ladi.	<b>shifrmtn</b>
97.	Kriptotizimning to'liq xavfsiz bo'lishi Kerxgofs prinsipiga ko'ra qaysi kattalikning nomalum bo'lishiga asoslanadi?	<b>Kalit</b>
98.	Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi?	<b>simmetrik va assimetrik turlarga</b>
99.	Kriptotahlil so'ziga berilgan to'g'ri tavsifni toping?	<b>Maxfiy shifrlarni buzish fani va sanati.</b>
100.	Kriptologiya so'ziga berilgan to'g'ri tavsifni toping?	<b>Maxfiy shifrlarni yaratish va buzish fani va sanati.</b>
101.	Kriptologiya qanday yo'nalishlarga bo'linadi?	<b>kriptografiya va kriptotahlil</b>
102.	Kriptografiya so'ziga berilgan to'g'ri tavsifni toping?	<b>Maxfiy shifrlarni yaratish fani va sanati.</b>
103.	Kompyuter viruslarini tarqalish usullarini ko'rsating?	<b>Ma'lumot saqlovchilari, Internetdan yuklab olish va elektron pochta orqali.</b>
104.	Kolliziya hodisasi deb nimaga aytiladi?	<b>ikki xil matn uchun bir xil xesh qiymat chiqishi</b>
105.	Kirish hujumlari bu?	<b>Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.</b>
106.	Kiberjinoyatchilik bu - ?	<b>Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.</b>
107.	Kiberetika bu - ?	<b>Kompyuterlar bilan bog'liq falsafiy soha bo'lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko'rsatishini o'rganadi.</b>
108.	Jumlani to'ldiring. Tizimli fikrlash ... uchun kerak.	<b>kafolatlangan amallarni ta'minlash</b>
109.	Jumlani to'ldiring. Tarmoqlararo ekranning vazifasi ...	<b>ishonchli va ishonchsiz tarmoqlar orasida ma'lumotlarga kirishni boshqarish.</b>
110.	Jumlani to'ldiring. Simmetrik shifrlash algoritmlari ochiq ma'lumotdan foydalanish tartibiga ko'ra ...	<b>blokli va oqimli turlarga bo'linadi.</b>
111.	Jumlani to'ldiring. Simli va simsiz tarmoqlar orasidagi asosiy farq ...	<b>tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud mavjudigi.</b>
112.	Jumlani to'ldiring. Sezar shifri akslantirishga asoslangan.....	<b>o'rniga qo'yish</b>
113.	Jumlani to'ldiring. Parol kalitdan farq qiladi.	<b>tasodifiylik darajasi bilan</b>
114.	Jumlani to'ldiring. Ma'lumotni uzatishda kriptografik himoya .....	<b>konfidensiallik va butunlikni ta'minlaydi.</b>
115.	Jumlani to'ldiring. Ma'lumotni konfidensialligini ta'minlash uchun.....zarur.	<b>shifrlash</b>
116.	Jumlani to'ldiring. Kriptografik himoya axborotning ... xususiyatini ta'minlamaydi.	<b>Foydalanuvchanlik</b>
117.	Jumlani to'ldiring. Hujumchi kabi fikrlash ... kerak.	<b>bo'lishi mumkin bo'lgan xavfni oldini olish uchun</b>
118.	Jumlani to'ldiring. Denial of service (DOS) hujumi axborotni ..... xususiyatini buzushga	<b>foydalanuvchanlik</b>

	qaratilgan.	
119.	Jumlani to'ldiring. Autentifikatsiya tizimlari asoslanishiga ko'ra ... turga bo'linadi.	<b>3</b>
120.	Jumlani to'ldiring. Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishiga olib kelsa.	<b>jinoyat sifatida baholanadi.</b>
121.	Jumlani to'ldiring shifrlar tasodifiy ketma-ketliklarni generatsiyalashga asoslanadi.	<b>Oqimli</b>
122.	Jumlani to'ldiring. .... - muhim bo'lgan axborot nusxalash yoki saqlash jarayoni bo'lib, bu ma'lumot yo'qolgan vaqtda qayta tiklash imkoniyatini beradi.	<b>Ma'lumotlarni zaxira nusxalash</b>
123.	Jumlani to'ldiring texnologiyasi lokal simsiz tarmoqlarga tegishli.	<b>WI-FI</b>
124.	Jumlani to'ldiring sohasi tashkil etuvchilar xavfsizligi, aloqa xavfsizligi va dasturiy ta'minotlar xavfsizligidan iborat.	<b>Tizim xavfsizligi</b>
125.	Jumlani to'ldiring kompyuter davriga tegishli shifrlarga misol bo'la oladi.	<b>DES, AES shifri</b>
126.	IPv6 protokolida IP manzilni ifodalashda necha bit ajratiladi.	<b>128</b>
127.	IP manzilni domen nomlariga yoki aksincha almashtirishni amalga oshiruvchi xizmat bu-	<b>DNS</b>
128.	Internet tarmog'idagi obro'sizlantirilgan kompyuterlar bu-?	<b>Botnet</b>
129.	Ikki kalitli kriptotizim bu -	<b>ochiq kalitli kriptotizim.</b>
130.	Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo'lgan murojaatlarini chegaralash qaysi himoya vositasining vazifasi hisoblanadi.	<b>Tarmoqlararo ekran.</b>
131.	Himoya mexanizmini aylanib o'tib tizimga ruxsatsiz kirish imkonini beruvchi zararli dastur turi bu?	<b>Backdoors</b>
132.	Har qanday vaziyatda biror bir hodisani yuzaga kelish ehtimoli qo'shilsa ....	<b>risk paydo bo'ladi.</b>
133.	Hajmi bo'yicha eng kichik hisoblangan tarmoq turi bu -	<b>PAN</b>
134.	GSM tarmog'ida ovozli so'zlashuvlarni shifrlash algoritmi bu?	<b>A5/1</b>
135.	GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating?	<b>A5/1</b>

136.	Foydalanuvchini tizimga tanitish jarayoni bu?	<b>Identifikatsiya</b>
137.	Foydalanuvchini haqiqiylikini tekshirish jarayoni bu?	<b>Autentifikatsiya</b>
138.	Foydalanuvchi tomonidan kiritilgan taqiqlangan so'rovni qaysi himoya vositasi yordamida nazoratlash mumkin.	<b>Tarmoqlararo ekran.</b>
139.	Foydalanuvchi parollari bazada qanday ko'rinishda saqlanadi?	<b>Xeshlangan ko'rinishda.</b>
140.	Foydalanuvchanlikni ta'minlash bu - ?	<b>ruxsatsiz bajarishdan himoyalash.</b>
141.	Fizik himoyani buzilishiga olib keluvchi tahdidlar yuzaga kelish shakliga ko'ra qanday guruhlariga bo'linadi?	<b>Tabiiy va sun'iy</b>
142.	Faqat simmetrik blokli shifrlarga xos bo'lgan atamani aniqlang?	<b>blok uzunligi</b>
143.	Faqat ob'ektning egasi tomonidan foydalanishga mos bo'lgan mantiqiy foydalanish usulini ko'rsating?	<b>Diskretsiyon foydalanishni boshqarish.</b>
144.	Faqat ma'lumotni butunligini ta'minlovchi kriptotizimlarni ko'rsating.	<b>MAC (Xabarlarini autentifikatsiya kodlari) tizimlari.</b>
145.	Faktorlash muammosi asosida yaratilgan assimetrik shifrlash usuli?	<b>RSA</b>
146.	Esda saqlashni va olib yurishni talab etmaydigan autentifikatsiya usuli bu -	<b>biometrik autentifikatsiya.</b>
147.	Eng zaif simsiz tarmoq protokolini ko'rsating?	<b>WEP</b>
148.	Elektron raqamli imzo muolajalarini ko'rsating?	<b>Imzoni shakllantirish va imkoni tekshirish.</b>
149.	Elektron ma'lumotlarni yo'q qilishda maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o'zgartiriladigan usul bu ...	<b>magnitsizlantirish</b>
150.	DNS serverlari tarmoqda qanday vazifani amalga oshiradi?	<b>Xost nomlari va internet nomlarini IP manzillarga o'zgartirish va teskarisini amalga oshiradi</b>
151.	Deshifrlash uchun kalit va kerak bo'ladi. ....	<b>shifrmavn</b>
152.	DES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?	<b>1</b>
153.	Buzg'unchiga xavfsizlik tizimini aylanib o'tib tizimga kirish imkonini beruvchi zararli dastur turi bu-?	<b>Backdoors</b>
154.	Biror narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilar tushuniladi.	<b>PIN, Parol.</b>
155.	Biror mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu-?	<b>Mantiqiy bombalar.</b>
156.	Biror faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami bu?	<b>Rol</b>
157.	Biba modeli axborotni qaysi xususiyatini ta'minlashni maqsad qiladi?	<b>Butunlik</b>
158.	Bell-Lapadula modeli axborotni qaysi xususiyatini ta'minlashni maqsad qiladi?	<b>Konfidensiallik</b>
159.	Axborotning konfidensialligi va butunligini ta'minlash uchun ikki uzil orasida himoyalangan tunelni quruvchi himoya vositasi bu?	<b>Virtual Private Network</b>
160.	Axborotni shifrlashdan maqsadi nima?	<b>Maxfiy xabar mazmunini yashirish.</b>
161.	Axborotni qaysi xususiyatlari simmetrik shifrlar yordamida ta'minlanadi.	<b>Konfidensiallik va butunlik.</b>
162.	Axborotni qaysi xususiyatlari ochiq kalitli shifrlar yordamida ta'minlanadi.	<b>Konfidensiallik</b>
163.	Axborotni mavjudligini yashirish bilan shug'ullanuvchi fan sohasi bu -	<b>steganografiya</b>
164.	Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ..... amalga oshiriladi.	<b>kodlash</b>
165.	Axborotni foydalanuvchanligini buzishga qaratilgan tahdidlar bu?	<b>DDOS tahdidlar.</b>
166.	Axborotni butunligini ta'minlash usullarini ko'rsating.	<b>Xesh funksiyalar, MAC.</b>
167.	Axborot xavfsizligida zaiflik bu?	<b>Tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson.</b>

168.	Axborot xavfsizligida tahdid bu?	<b>Aktivga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.</b>
169.	Axborot xavfsizligida risk bu?	<b>Manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta'sirida tahdid qilish ehtimoli.</b>
170.	Axborot xavfsizligida boshqarish vositasi bu?	<b>Natijasi zaiflik yoki tahdidga ta'sir qiluvchi riskni o'zgartiradigan harakatlar.</b>
171.	Axborot xavfsizligida aktiv bu?	<b>Tashkilot yoki foydalanuvchi uchun qadrlı bo'lgan ixtiyoriy narsa.</b>
172.	Axborot saqlagich vositalaridan qayta foydalanish xususiyatini saqlab qolgan holda axborotni yo'q qilish usuli qaysi?	<b>Bir necha marta takroran yozish va maxsus dasturlar yordamida saqlagichni tozalash</b>
173.	Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?	<b>2 ta</b>
174.	Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating?	<b>Paydo bo'layotgan zararli dasturiy vositalar sonining ko'pligi.</b>
175.	Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating?	<b>Paydo bo'layotgan zararli dasturiy vositalar sonining ko'pligi.</b>
176.	Agar simmetrik kalitning uzunligi 64 bit bo'lsa, jami bo'lishi mumkin bo'lgan kalitlar soni nechta?	<b><math>2^{64}</math></b>
177.	Agar parolning uzunligi 8 ta belgi va har bir o'rinda 128 ta turlicha belgidan foydalanish mumkin bo'lsa, bo'lishi mumkin bo'lgan jami parollar sonini toping.	<b><math>128^8</math></b>
178.	Agar ob'ektning xavfsizlik darajasi sub'ektning xavfsizlik darajasidan kichik yoki teng bo'lsa, u holda O'qish uchun ruxsat beriladi. Ushbu qoida qaysi foydalanishni boshqarish usuliga tegishli.	<b>MAC</b>
179.	AES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?	<b>1</b>
180.	A5/1 shifri qaysi turga mansub?	<b>oqimli shifrlar</b>
181.	A5/1 shifri bu -	<b>oqimli shifr.</b>
182.	A5/1 oqimli shifrlash algoritmda maxfiy kalit necha registrga bo'linadi?	<b>3</b>
183.	A5/1 oqimli shifrlash algoritmda dastlabki kalit uzunligi nechı bitga teng?	<b>64</b>
184.	A5/1 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi?	<b>mobil aloqa standarti GSM protokolida</b>
185.	A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?	<b>1</b>
186.	9 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?	<b>10, 8</b>
187.	64 ta belgidan iborat Sezar shifrlash usulida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin?	<b>63</b>
188.	2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo'yicha qo'shing?	<b>00001</b>
189.	2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo'yicha qo'shing?	<b>00001</b>
190.	2 lik sanoq tizimida 11011 soniga 00100 sonini 2 modul bo'yicha qo'shing?	<b>11111</b>
191.	13 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?	<b>5, 7</b>
192.	12 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?	<b>11, 13</b>
193.	... umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi.	<b>Tarmoqlararo ekran</b>
194.	... umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi.	<b>Tarmoqlararo ekran</b>



<b>195.</b>	“Yelka orqali qarash” hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.	<b>Parolga asoslangan autentifikatsiya.</b>
<b>196.</b>	..... hujumida hujumchi o‘rnatilgan aloqaga suqilib kiradi va aloqani bo‘ladi. Nuqtalar o‘rniga mos javobni qo‘ying.	<b>O‘rtada turgan odam.</b>
<b>197.</b>	..... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to‘plami.	<b>Alifbo</b>
<b>198.</b>	.... shifrlar blokli va oqimli turlarga ajratiladi	<b>simmetrik</b>
<b>199.</b>	.... kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi.	<b>Kriptografik kalit</b>
<b>200.</b>	.... kriptografik shifrlash algoritmlari blokli va oqimli turlarga ajratiladi.	<b>Simmetrik</b>