Axborot xavfsizligi yo’nalishi bakalavr talabalari uchun “Kiberxavfsizlik” fanidan

TESTLAR

№	Test topshirig’i	To’g’ri javob	Muqobil javob	Muqobil javob	Muqobil javob	
1.	Konfidensiallikni ta’minlash bu - ?	ruxsatsiz o‘qishdan himoyalash.	ruxsatsiz yozishdan himoyalash.	ruxsatsiz bajarishdan himoyalash.	ruxsat etilgan amallarni bajarish.	1
2.	Foydalanuvchanlikni ta’minlash bu - ?	ruxsatsiz bajarishdan himoyalash.	ruxsatsiz yozishdan himoyalash.	ruxsatsiz o‘qishdan himoyalash.	ruxsat etilgan amallarni bajarish.	1
3.	Yaxlitlikni ta’minlash bu - ?	ruxsatsiz yozishdan himoyalash.	ruxsatsiz o‘qishdan himoyalash.	ruxsatsiz bajarishdan himoyalash.	ruxsat etilgan amallarni bajarish.	1
4.	Jumlani to‘ldiring. Hujumchi kabi fikrlash ... kerak.	bo‘lishi mumkin bo‘lgan xavfni oldini olish uchun	kafolatlangan amallarni ta’minlash uchun	ma’lumot, axborot va tizimdan foydalanish uchun	ma’lumotni aniq va ishonchli ekanligini bilish uchun	1
5.	Jumlani to‘ldiring. Tizimli fikrlash ... uchun kerak.	kafolatlangan amallarni ta’minlash	bo‘lishi mumkin bo‘lgan xavfni oldini olish	ma’lumot, axborot va tizimdan foydalanish	ma’lumotni aniq va ishonchli ekanligini bilish	1
6.	Axborot xavfsizligida risk bu?	Manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta’sirida tahdid qilish ehtimoli.	U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz.	Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa.	Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.	1
7.	Axborot xavfsizligida tahdid bu?	Aktivga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.	Noaniqlikning maqsadlarga ta’siri.	U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz.	Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa.	1
8.	Axborot xavfsizligida aktiv bu?	Tashkilot yoki foydalanuvchi uchun qadrli bo‘lgan ixtiyoriy narsa.	Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.	Noaniqlikning maqsadlarga ta’siri.	U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz.	1
9.	Axborot xavfsizligida zaiflik bu?	Tahdidga sabab bo‘luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson.	Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa.	Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.	Noaniqlikning maqsadlarga ta’siri.	1
10.	Axborot xavfsizligida boshqarish vositasi bu?	Natijasi zaiflik yoki tahdidga ta’sir qiluvchi riskni o‘zgartiradigan harakatlar.	Bir yoki bir nechta tahdidga sabab bo‘luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik.	Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa.	Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.	1
11.	Har qanday vaziyatda biror bir hodisani yuzaga kelish ehtimoli qo‘shilsa	risk paydo bo‘ladi.	hujum paydo bo‘ladi.	tahdid paydo bo‘ladi.	aktiv paydo bo‘ladi.	1
12.	Jumlani to‘ldiring. Denial of service (DOS) hujumi axborotni .... xususiyatini buzushga qaratilgan.	foydalanuvchanlik	butunlik	konfidensiallik	ishonchlilik	1
13.	Jumlani to‘ldiring. ... sohasi tashkil etuvchilar xavfsizligi, aloqa xavfsizligi va dasturiy ta’minotlar xavfsizligidan iborat.	Tizim xavfsizligi	Ma’lumotlar xavfsizligi	Inson xavfsizligi	Tashkilot xavfsizligi	1
14.	Kriptologiya so‘ziga berilgan to‘g‘ri tavsifni toping?	Maxfiy shifrlarni yaratish va buzish fani va sanati.	Maxfiy shifrlarni yaratish fani va sanati.	Maxfiy shifrlarni buzish fani va sanati.	Axborotni himoyalash fani va sanati.	1
15.	.... kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi.	Kriptografik kalit	Ochiq matn	Alifbo	Algoritm	1
16.	Kriptografiya so‘ziga berilgan to‘g‘ri tavsifni toping?	Maxfiy shifrlarni yaratish fani va sanati.	Maxfiy shifrlarni yaratish va buzish fani va sanati.	Maxfiy shifrlarni buzish fani va sanati.	Axborotni himoyalash fani va sanati.	1
17.	Kriptotahlil so‘ziga berilgan to‘g‘ri tavsifni toping?	Maxfiy shifrlarni buzish fani va sanati.	Maxfiy shifrlarni yaratish fani va sanati.	Maxfiy shifrlarni yaratish va buzish fani va sanati.	Axborotni himoyalash fani va sanati.	1
18.	..... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to‘plami.	Alifbo	Ochiq matn	Shifrmatn	Kodlash	1

19.	Ma’lumot shifrlansa, natijasi .... bo‘ladi.	shifrmatn	ochiq matn	nomalum	kod	1
20.	Deshifrlash uchun kalit va ..... kerak bo‘ladi.	shifrmatn	ochiq matn	kodlash	alifbo	1
21.	Ma’lumotni shifrlash va deshifrlashda yagona kalitdan foydalanuvchi tizim bu -	simmetrik kriptotizim.	ochiq kalitli kriptotizim.	asimetrik kriptotizim.	xesh funksiyalar.	1
22.	Ikki kalitli kriptotizim bu -	ochiq kalitli kriptotizim.	simmetrik kriptotizim.	xesh funksiyalar.	MAC tizimlari.	1
23.	Axborotni mavjudligini yashirish bilan shug‘ullanuvchi fan sohasi bu -	steganografiya.	kriptografiya.	kodlash.	kriptotahlil.	1
24.	Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ..... amalga oshiriladi.	kodlash	shifrlash	yashirish	deshifrlash	1
25.	Jumlani to‘ldiring. Ma’lumotni konfidensialligini ta’minlash uchun ..... zarur.	shifrlash	kodlash	dekodlash	deshifrlash	1
26.	Ma’lumotni mavjudligini yashirishda	steganografik algoritmdan foydalaniladi.	kriptografik algoritmdan foydalaniladi.	kodlash algoritmidan foydalaniladi.	kriptotahlil algoritmidan foydalaniladi.	1
27.	Xesh funksiyalar - .... funksiya.	kalitsiz kriptografik	bir kalitli kriptografik	ikki kalitli kriptografik	ko‘p kalitli kriptografik	1
28.	Jumlani to‘ldiring. Ma’lumotni uzatishda kriptografik himoya	konfidensiallik va butunlikni ta’minlaydi.	konfidensiallik va foydalanuvchanlikni ta’minlaydi.	foydalanuvchanlik va butunlikni ta’minlaydi.	konfidensiallik ta’minlaydi.	1
29.	Jumlani to‘ldiring. ... kompyuter davriga tegishli shifrlarga misol bo‘la oladi.	DES, AES shifri	Sezar shifri	Kodlar kitobi	Enigma shifri	1
30.	.... kriptografik shifrlash algoritmlari blokli va oqimli turlarga ajratiladi.	Simmetrik	Ochiq kalitli	Asimmetrik	Klassik davr	1
31.	Jumlani to‘ldiring. .... shifrlar tasodifiy ketma-ketliklarni generatsiyalashga asoslanadi.	Oqimli	Blokli	Ochiq kalitli	Asimetrik	1
32.	Ochiq matn qismlarini takroriy shifrlovchi algoritmlar bu -	blokli shifrlar	oqimli shifrlash	ochiq kalitli shifrlar	asimmetrik shifrlar	1
33.	A5/1 shifri bu -	oqimli shifr.	blokli shifr.	ochiq kalitli shifr.	asimmetrik shifr	1
34.	Quyidagi muammolardan qaysi biri simmetrik kriptotizimlarga xos.	Kalitni taqsimlash zaruriyati.	Shifrlash jarayonining ko‘p vaqt olishi.	Kalitlarni esda saqlash murakkabligi.	Foydalanuvchilar tomonidan maqbul ko‘rilmasligi.	1
35.	Quyidagi atamalardan qaysi biri faqat simmetrik blokli shifrlarga xos?	Blok uzunligi.	Kalit uzunligi.	Ochiq kalit.	Kodlash jadvali.	1
36.	Jumlani to‘ldiring. Sezar shifri .... akslantirishga asoslangan.	o‘rniga qo‘yish	o‘rin almashtirish	ochiq kalitli	kombinatsion	1
37.	Kriptotizimning to‘liq xavfsiz bo‘lishi Kerxgofs prinsipiga ko‘ra qaysi kattalikning nomalum bo‘lishiga asoslanadi?	Kalit.	Algoritm.	Shifrmatn.	Protokol.	1
38.	Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi shifrlar bu -	ochiq kalitli shifrlar.	simmetrik shifrlar.	bir kalitli shifrlar	xesh funksiyalar.	1
39.	Agar simmetrik kalitning uzunligi 64 bit bo‘lsa, jami bo‘lishi mumkin bo‘lgan kalitlar soni nechta?	2^{64}	64!	64^2	2^{63}	1
40.	Axborotni qaysi xususiyatlari simmetrik shifrlar yordamida ta’minlanadi.	Konfidensiallik va butunlik.	Konfidensiallik.	Butunlik va foydalanuvchanlik.	Foydalanuvchanlik va konfidensiallik.	1
41.	Axborotni qaysi xususiyatlari ochiq kalitli	Konfidensiallik.	Konfidensiallik, butunlik va	Butunlik va foydalanuvchanlik.	Foydalanuvchanlik va konfidensiallik.	1

	shifrlar yordamida ta’minlanadi.		foydalanuvchanlik.			
42.	Quyidagilardan qaysi biri rad etishdan himoyani ta’minlaydi.	Elektron raqamli imzo tizimi.	MAC tizimlari.	Simmetrik shifrlash tizimlari.	Xesh funksiyalar.	1
43.	Qaysi ochiq kalitli algoritm katta sonni faktorlash muammosiga asoslanadi?	RSA algoritmi.	El-Gamal algoritmi.	DES.	TEA.	1
44.	Rad etishdan himoyalashda ochiq kalitli kriptotizimlarning qaysi xususiyati muhim hisoblanadi.	Ikkita kalitdan foydalanilgani.	Matematik muammoga asoslanilgani.	Ochiq kalitni saqlash zaruriyati mavjud emasligi.	Shaxsiy kalitni saqlash zarurligi.	1
45.	Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas.	Bir tomonlama funksiya bo‘lmasligi kerak.	Amalga oshirishdagi yuqori tezkorlik.	Turli kirishlar turli chiqishlarni akslantirishi.	Kolliziyaga bardoshli bo‘lishi.	1
46.	Quyidagi xususiyatlardan qaysi biri elektron raqamli imzo tomonidan ta’minlanadi?	Axborot butunligini va rad etishdan himoyalash.	Axborot konfidensialligini va rad etishdan himoyalash.	Axborot konfidensialligi.	Axborot butunligi.	1
47.	Faqat ma’lumotni butunligini ta’minlovchi kriptotizimlarni ko‘rsating.	MAC (Xabarlarni autentifikatsiya kodlari) tizimlari.	Elektron raqamli imzo tizimlari.	Ochiq kalitli kriptografik tizimlar.	Barcha javoblar to‘g‘ri.	1
48.	Foydalanuvchini tizimga tanitish jarayoni bu?	Identifikatsiya.	Autentifikatsiya.	Avtorizatsiya.	Ro‘yxatga olish.	1
49.	Foydalanuvchini haqiqiyligini tekshirish jarayoni bu?	Autentifikatsiya.	Identifikatsiya.	Avtorizatsiya.	Ro‘yxatga olish.	1
50.	Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu?	Avtorizatsiya.	Autentifikatsiya.	Identifikatsiya.	Ro‘yxatga olish.	1
51.	Parolga asoslangan autentifikatsiya usulining asosiy kamchiligini ko‘rsating?	Esda saqlash zaruriyati.	Birga olib yurish zaririyati.	Almashtirib bo‘lmaslik.	Qalbakilashtirish mumkinligi.	1
52.	Biror narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilar tushuniladi.	PIN, Parol.	Token, mashinaning kaliti.	Yuz tasviri, barmoq izi.	Biometrik parametrlar.	1
53.	Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting?	Doimo xavfsiz saqlab olib yurish zaruriyati.	Doimo esada saqlash zaruriyati.	Qalbakilashtirish muammosi mavjudligi.	Almashtirib bo‘lmaslik.	1
54.	Esda saqlashni va olib yurishni talab etmaydigan autentifikatsiya usuli bu -	biometrik autentifikatsiya.	parolga asoslangan autentifikatsiya.	tokenga asoslangan autentifikatsiya.	ko‘p faktorli autentifikatsiya.	1
55.	Qaysi biometrik parametr eng yuqori universallik xususiyatiga ega?	Yuz tasviri.	Ko‘z qorachig‘i.	Barmoq izi.	Qo‘l shakli.	1
56.	Qaysi biometrik parametr eng yuqori takrorlanmaslik xususiyatiga ega?	Ko‘z qorachig‘i.	Yuz tasviri.	Barmoq izi.	Qo‘l shakli.	1
57.	Quyidagilardan qaysi biri har ikkala tomonning haqiqiyligini tekshirish jarayonini ifodalaydi?	Ikki tomonlama autentifikatsiya.	Ikki faktorli autentifikatsiya.	Ko‘p faktorli autentifikatsiya.	Biometrik autentifikatsiya.	1
58.	Parolga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko‘rsating?	Parollar lug‘atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum.	Fizik o‘g‘irlash hujumi, yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum.	Parollar lug‘atidan foydalanish asosida hujum, yelka orqali qarash hujumi, qalbakilashtirish hujumi.	Parollar lug‘atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararli dasturlardan foydanish asosida hujum.	1
59.	Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko‘rsating?	Fizik o‘g‘irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar	Parollar lug‘atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum	Fizik o‘g‘irlash, yelka orqali qarash hujumi, zararli dasturlardan foydalanishga asoslangan hujumlar	Parollar lug‘atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararli dasturlardan foydalanish asosida hujum	1

60.	Foydalanuvchi parollari bazada qanday ko‘rinishda saqlanadi?	Xeshlangan ko‘rinishda.	Shifrlangan ko‘rinishda.	Ochiq holatda.	Bazada saqlanmaydi.	1
61.	Agar parolning uzunligi 8 ta belgi va har bir o‘rinda 128 ta turlicha belgidan foydalanish mumkin bo‘lsa, bo‘lishi mumkin bo‘lgan jami parollar sonini toping.	128^8	8^{128}	128!	2^{128}	1
62.	Parolni “salt” (tuz) kattaligidan foydalanib xeshlashdan (h(password, salt)) asosiy maqsad nima?	Buzg‘unchiga ortiqcha hisoblashni talab etuvchi murakkablikni yaratish.	Buzg‘unchi topa olmasligi uchun yangi nomalum kiritish.	Xesh qiymatni tasodifiylik darajasini oshirish.	Xesh qiymatni qaytmaslik talabini oshirish.	1
63.	Quyidagilardan qaysi biri tabiy tahdidga misol bo‘ladi?	Yong‘in, suv toshishi, harorat ortishi.	Yong‘in, o‘g‘irlik, qisqa tutashuvlar.	Suv toshishi, namlikni ortib ketishi, bosqinchilik.	Bosqinchilik, terrorizm, o‘g‘irlik.	1
64.	Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan?	Ma’muriy nazoratlash.	Fizik nazoratlash.	Texnik nazoratlash.	Apparat nazoratlash.	1
65.	Faqat ob’ektning egasi tomonidan foydalanishga mos bo‘lgan mantiqiy foydalanish usulini ko‘rsating?	Diskretsion foydalanishni boshqarish.	Mandatli foydalanishni boshqarish.	Rolga asoslangan foydalanishni boshqarish.	Attributga asoslangan foydalanishni boshqarish.	1
66.	Qaysi usul ob’ektlar va sub’ektlarni klassifikatsiyalashga asoslangan?	Mandatli foydalanishni boshqarish.	Diskretsion foydalanishni boshqarish.	Rolga asoslangan foydalanishni boshqarish.	Attributga asoslangan foydalanishni boshqarish.	1
67.	Biror faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami bu?	Rol.	Imtiyoz.	Daraja.	Imkoniyat.	1
68.	Qoida, siyosat, qoida va siyosatni mujassamlashtirgan algoritmlar, majburiyatlar va maslahatlar kabi tushunchalar qaysi foydalanishni boshqarish usuliga aloqador.	Attributga asoslangan foydalanishni boshqarish.	Rolga asoslangan foydalanishni boshqarish.	Mandatli foydalanishni boshqarish.	Diskretsion foydalanishni boshqarish.	1
69.	Bell-Lapadula modeli axborotni qaysi xususiyatini ta’minlashni maqsad qiladi?	Konfidensiallik.	Butunlik.	Foydalanuvchanlik.	Ishonchlilik.	1
70.	Biba modeli axborotni qaysi xususiyatini ta’minlashni maqsad qiladi?	Butunlik.	Konfidensiallik.	Foydalanuvchanlik.	Maxfiylik.	1
71.	Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi?	Apparat.	Dasturiy.	Simmetrik.	Ochiq kalitli.	1
72.	Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalanadi?	Dasturiy.	Apparat.	Simmetrik.	Ochiq kalitli.	1
73.	Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko‘rsating?	Ochiq kalitli shifrlar.	Simmetrik shifrlar.	Blokli shifrlar.	Oqimli shifrlar.	1
74.	Xesh funksiyalarda kolliziya hodisasi bu?	Ikki turli matnlarning xesh qiymatlarini bir xil bo‘lishi.	Cheksiz uzunlikdagi axborotni xeshlay olishi.	Tezkorlikda xeshlash imkoniyati.	Turli matnlar uchun turli xesh qiymatlarni hosil bo‘lishi.	1
75.	64 ta belgidan iborat Sezar shifrlash usilida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin?	63	63!	32	32^2	1

76.	Elektron raqamli imzo muolajalarini ko‘rsating?	Imzoni shakllantirish va imkoni tekshirish.	Shifrlash va deshifrlash.	Imzoni xeshlash va xesh matnni deshifrlash.	Imzoni shakllartirish va xeshlash.	1
77.	“Yelka orqali qarash” hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.	Parolga asoslangan autentifikatsiya.	Tokenga asoslangan autentifikatsiya.	Biometrik autentifikatsiya.	Ko‘z qorachig‘iga asoslangan autentifikatsiya.	1
78.	Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan.	Parolga asoslangan autentifikatsiya.	Tokenga asoslangan autentifikatsiya.	Biometrik autentifikatsiya.	Ko‘z qorachig‘iga asoslangan autentifikatsiya.	1
79.	Yo‘qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon.	Parolga asoslangan autentifikatsiya.	Tokenga asoslangan autentifikatsiya.	Biometrik autentifikatsiya.	Ko‘z qorachig‘iga asoslangan autentifikatsiya.	1
80.	Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.	Biometrik autentifikatsiya.	Biror narsani bilishga asoslangan autentifikatsiya.	Biror narsaga egalik qilishga asoslangan autentifikatsiya.	Tokenga asoslangan autentifikatsiya	1
81.	Axborotni butunligini ta’minlash usullarini ko‘rsating.	Xesh funksiyalar, MAC.	Shifrlash usullari.	Assimetrik shifrlash usullari, CRC tizimlari.	Shifrlash usullari, CRC tizimlari.	1
82.	Quyidagilardan qaysi biri to‘liq kompyuter topologiyalarini ifodalamaydi.	LAN, GAN, OSI.	Yulduz, WAN, TCP/IP.	Daraxt, IP, OSI.	Shina, UDP, FTP.	1
83.	OSI tarmoq modeli nechta sathdan iborat?	7	4	6	5	1
84.	TCP/IP tarmoq modeli nechta sathdan iborat?	4	7	6	5	1
85.	Hajmi bo‘yicha eng kichik hisoblangan tarmoq turi bu -	PAN	LAN	CAN	MAN	1
86.	IPv6 protokolida IP manzilni ifodalashda necha bit ajratiladi.	128	32	64	4	1
87.	IP manzilni domen nomlariga yoki aksincha almashtirishni amalga oshiruvchi xizmat bu-	DNS	TCP/IP	OSI	UDP	1
88.	Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi hodisalarning potensial paydo bo‘lishi bu?	Tahdid.	Zaiflik.	Hujum.	Aktiv.	1
89.	Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat bu?	Hujum.	Zaiflik.	Tahdid.	Zararli harakat.	1
90.	Quyidagilardan qaysi biri tarmoq xavfsizligi muammolariga sabab bo‘lmaydi?	Routerlardan foydalanmaslik.	Qurilma yoki dasturiy vositani noto‘g‘ri sozlanish.	Tarmoqni xavfsiz bo‘lmagan tarzda va zaif loyihalash.	Tug‘ma texnologiya zaifligi.	1
91.	Tarmoq xavfsizligini buzulishi biznes faoliyatga qanday ta’sir qiladi?	Biznes faoliyatning buzilishi, huquqiy javobgarlikka sababchi bo‘ladi.	Axborotni o‘g‘irlanishi, tarmoq qurilmalarini fizik buzilishiga olib keladi.	Maxfiylikni yo‘qolishi, tarmoq qurilmalarini fizik buzilishiga olib keladi.	Huquqiy javobgarlik, tarmoq qurilmalarini fizik buzilishiga olib keladi.	1
92.	Razvedka hujumlari bu?	Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi.	Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.	Foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi.	Tizimni fizik buzishni maqsad qiladi.	1
93.	Kirish hujumlari bu?	Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.	Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi.	Foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi.	Tarmoq haqida axborotni to‘plash hujumchilarga mavjud bo‘lgan potensial zaiflikni aniqlashga harakat qiladi.	1
94.	Xizmatdan vos kechishga	Foydalanuvchilarga	Turli	Asosiy hujumlarni	Tarmoq haqida	1

	qaratilgan hujumlar bu?	va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi.	texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.	oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi.	axborotni to‘plash hujumchilarga mavjud bo‘lgan potensial zaiflikni aniqlashga harakat qiladi.	
95.	Paketlarni snifferlash, portlarni skanerlash va Ping buyrug‘ini yuborish hujumlari qaysi hujumlar toifasiga kiradi?	Razvedka hujumlari.	Kirish hujumlari.	DOS hujumlari.	Zararli dasturlar yordamida amalga oshiriladigan hujumlar.	1
96.	O‘zini yaxshi va foydali dasturiy vosita sifatida ko‘rsatuvchi zararli dastur turi bu?	Troyan otlari.	Adware.	Spyware.	Backdoors.	1
97.	Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi zararli dastur turi bu?	Adware.	Troyan otlari.	Spyware.	Backdoors.	1
98.	Himoya mexanizmini aylanib o‘tib tizimga ruxsatsiz kirish imkonini beruvchi zararli dastur turi bu?	Backdoors.	Adware.	Troyan otlari.	Spyware.	1
99.	Paket filterlari turidagi tarmoqlararo ekran vositasi OSI modelining qaysi sathida ishlaydi?	Tarmoq sathida.	Transport sathida.	Ilova sathida.	Kanal sathida.	1
100	Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi.	Tarmoqlararo ekran.	Antivirus.	Virtual himoyalangan tarmoq.	Router.	1
101	Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo‘lgan murojaatlarini chegaralash qaysi himoya vositasining vazifasi hisoblanadi.	Tarmoqlararo ekran.	Antivirus.	Virtual himoyalangan tarmoq.	Router.	1
102	2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo‘yicha qo‘shing?	00001	10000	01100	11111	1
103	2 lik sanoq tizimida 11011 soniga 00100 sonini 2 modul bo’yicha qo’shing?	11111	10101	11100	01001	1
104	2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo’yicha qo’shing?	00001	10000	01100	11111	1
105	Axborot saqlagich vositalaridan qayta foydalanish xususiyatini saqlab qolgan holda axborotni yo’q qilish usuli qaysi?	Bir necha marta takroran yozish va maxsus dasturlar yordamida saqlagichni tozalash	Magnitsizlantirish	Formatlash	Axborotni saqlagichdan o’chirish	1
106	Elektron ma’lumotlarni yo’q qilishda maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o’zgartiriladigan usul bu ...	magnitsizlantirish.	shredirlash.	yanchish.	formatlash.	1
107	Yo’q qilish usullari orasidan ekologik jihatdan ma’qullanmaydigan va maxsus joy talab qiladigan usul qaysi?	Yoqish	Maydalash	Ko’mish	Kimyoviy ishlov berish	1
108	Kiberjinoyatchilik bu - ?	Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa	Kompyuterlar bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning	Hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud	Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti.	1

		qurilmalar orqali qilingan jinoiy faoliyat.	xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta’sir ko‘rsatishini o‘rganadi.	bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.		
109	Kiberetika bu - ?	Kompyuterlar bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta’sir ko‘rsatishini o‘rganadi.	Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.	Hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.	Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti.	1
110	Shaxsiy simsiz tarmoqlar qo‘llanish sohasini belgilang	Tashqi qurilmalar kabellarining o‘rnida	Binolar va korxonalar va internet orasida belgilangan simsiz bog‘lanish	Butun dunyo bo‘yicha internetdan foydalanishda	Simli tarmoqlarni mobil kengaytirish	1
111	VPNning texnik yechim arxitekturasiga ko’ra turlari keltirilgan qatorni aniqlang?	Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN; korporativ tarmoqlararo VPN	Kanal sathidagi VPN; tarmoq sathidagi VPN; seans sathidagi VPN	Marshuritizator ko’rinishidagi VPN; tramoqlararo ekran ko’rinishidagi VPN	Dasturiy ko’rinishdagi VPN; maxsus shifrlash protsessoriga ega apparat vosita ko’rinishidagi VPN	1
112	Axborotning konfidensialligi va butunligini ta’minlash uchun ikki uzel orasida himoyalangan tunelni quruvchi himoya vositasi bu?	Virtual Private Network	Firewall	Antivirus	IDS	1
113	Qanday tahdidlar passiv hisoblanadi?	Amalga oshishida axborot strukturasi va mazmunida hech narsani o‘zgartirmaydigan tahdidlar	Hech qachon amalga oshirilmaydigan tahdidlar	Axborot xavfsizligini buzmaydigan tahdidlar	Texnik vositalar bilan bog‘liq bo‘lgan tahdidlar	1
114	Quyidagi qaysi hujum turi razvedka hujumlari turiga kirmaydi?	Ddos	Paketlarni snifferlash	Portlarni skanerlash	Ping buyrug‘ini yuborish	1
115	Trafik orqali axborotni to’plashga harakat qilish razvedka hujumlarining qaysi turida amalga oshiriladi?	Passiv	DNS izi	Lug’atga asoslangan	Aktiv	1
116	Portlarni va operatsion tizimni skanerlash razvedka hujumlarining qaysi turida amalga oshiriladi?	Aktiv	Passiv	DNS izi	Lug’atga asoslangan	1
117	Paketlarni snifferlash, portlarni skanerlash, ping buyrug’ini yuborish qanday hujum turiga misol bo’ladi?	Razvedka hujumlari	Xizmatdan voz kechishga undash hujumlari	Zararli hujumlar	Kirish hujumlari	1
118	DNS serverlari tarmoqda qanday vazifani amalga oshiradi?	Xost nomlari va internet nomlarini IP manzillarga o’zgartirish va teskarisini amalga oshiradi	Ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq uchun kiruvchi nuqta vazifasini bajaradi	Tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq uchun chiqish nuqtasi vazifasini bajaradi	Internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlash funksiyasini amalga oshiradi	1
119	Markaziy xab yoki tugun orqali tarmoqni markazlashgan holda boshqarish qaysi tarmoq topologiyasida amalga	Yulduz	Shina	Xalqa	Mesh	1

	oshiriladi?					
120	Quyidagilardan qaysilari ananaviy tarmoq turi hisoblanadi?	WAN, MAN, LAN	OSI, TCP/IP	UDP, TCP/IP, FTP	Halqa, yulduz, shina, daraxt	1
121	Quyidagilardan qaysilari tarmoq topologiyalari hisoblanadi?	Halqa, yulduz, shina, daraxt	UDP, TCP/IP, FTP	OSI, TCP/IP	SMTP, HTTP, UDP	1
122	Yong'inga qarshi tizimlarni aktiv chora turiga quyidagilardan qaysilari kiradi?	Yong'inni aniqlash va bartaraf etish tizimi	Minimal darajada yonuvchan materiallardan foydalanish	Yetarlicha miqdorda qo'shimcha chiqish yo'llarini mavjudligi	Yong'inga aloqador tizimlarni to'g'ri madadlanganligi	1
123	Yong‘inga qarshi kurashishning aktiv usuli to‘g‘ri ko‘rsatilgan javobni toping?	Tutunni aniqlovchilar, alangani aniqlovchilar va issiqlikni aniqlovchilar	Binoga istiqomat qiluvchilarni yong‘in sodir bo‘lganda qilinishi zarur bo‘lgan ishlar bilan tanishtirish	Minimal darajada yonuvchan materiallardan foydalanish, qo‘shimcha etaj va xonalar qurish	Yetarli sondagi qo‘shimcha chiqish yo‘llarining mavjudligi	1
124	Yong‘inga qarshi kurashishning passiv usuliga kiruvchi choralarni to‘g‘ri ko‘rsatilgan javobni toping?	Minimal darajada yonuvchan materiallardan foydalanish, qo‘shimcha etaj va xonalar qurish	Tutun va alangani aniqlovchilar	O‘t o'chirgich, suv purkash tizimlari	Tutun va alangani aniqlovchilar va suv purkash tizimlari	1
125	Fizik himoyani buzilishiga olib keluvchi tahdidlar yuzaga kelish shakliga ko‘ra qanday guruhlarga bo‘linadi?	Tabiy va sun'iy	Ichki va tashqi	Aktiv va passiv	Bir faktorlik va ko‘p faktorli	1
126	Quyidagilarnnig qaysi biri tabiiy tahdidlarga misol bo'la oladi?	Toshqinlar, yong'in, zilzila	Bosqinchilik, terrorizm, o‘g‘irlik	O'g'irlik, toshqinlar, zilzila	Terorizim, toshqinlar, zilzila	1
127	Quyidagilarnnig qaysi biri sun'iy tahdidlarga misol bo'la oladi?	Bosqinchilik, terrorizm, o‘g‘irlik	Toshqinlar, zilzila, toshqinlar	O'g'irlik, toshqinlar, zilzila	Terorizim, toshqinlar, zilzila	1
128	Kolliziya hodisasi deb nimaga aytiladi?	ikki xil matn uchun bir xil xesh qiymat chiqishi	ikki xil matn uchun ikki xil xesh qiymat chiqishi	bir xil matn uchun bir xil xesh qiymat chiqishi	bir xil matn uchun ikki xil xesh qiymat chiqishi	1
129	GSM tarmog‘ida foydanalaniluvchi shifrlash algoritmi nomini ko‘rsating?	A5/1	DES	AES	RC4	1
130	O‘zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko‘rsating?	“UNICON.UZ” DUK	“O‘zstandart” agentligi	Davlat Soliq Qo‘mitasi	Kadastr agentligi	1
131	RC4 shifrlash algoritmi simmetrik turga mansub bo‘lsa, unda nechta kalitdan foydalaniladi?	1	2	3	4	1
132	A5/1 shifrlash algoritmi simmetrik turga mansub bo‘lsa, unda nechta kalitdan foydalaniladi?	1	2	3	4	1
133	AES shifrlash algoritmi simmetrik turga mansub bo‘lsa, unda nechta kalitdan foydalaniladi?	1	2	3	4	1
134	DES shifrlash algoritmi simmetrik turga mansub bo‘lsa, unda nechta kalitdan foydalaniladi?	1	2	3	4	1
135	A5/1 oqimli shifrlash algoritmida maxfiy kalit necha registrga bo'linadi?	3	4	5	6	1
136	Faqat simmetrik blokli shifrlarga xos bo‘lgan atamani aniqlang?	blok uzunligi	kalit uzunligi	ochiq kalit	kodlash jadvali	1
137	A5/1 shifri qaysi turga mansub?	oqimli shifrlar	blokli shifrlar	ochiq kalitli shifrlar	assimetrik shifrlar	1
138	.... shifrlar blokli va oqimli turlarga ajratiladi	simmetrik	ochiq kalitli	assimetrik	klassik	1
139	Quyida keltirilgan	ixtiyoriy olingan har	ixtiyoriy olingan bir	ixtiyoriy olingan har	ixtiyoriy olingan har xil	1

	xususiyatlarning qaysilari xesh funksiyaga mos?	xil matn uchun xesh qiymatlar bir xil bo‘lmaydi	xil matn uchun qiymatlar bir xil bo‘lmaydi	xil matn uchun xesh qiymatlar bir xil bo‘ladi	xesh qiymat uchun dastlabki ma’lumotlar bir xil bo‘ladi	
140	Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?	chiqishda fiksirlangan uzunlikdagi qiymatni beradi	chiqishda bir xil qiymatni beradi	chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo‘ladi	kolliziyaga ega	1
141	Xesh qiymatlarni yana qanday atash mumkin?	dayjest	funksiya	imzo	raqamli imzo	1
142	A5/1 oqimli shifrlash algoritmida dastlabki kalit uzunligi nechi bitga teng?	64	512	192	256	1
143	A5/1 oqimli shifrlash algoritmi asosan qayerda qo‘llaniladi?	mobil aloqa standarti GSM protokolida	simsiz aloqa vositalaridagi mavjud WEP protokolida	internet trafiklarini shifrlashda	radioaloqa tarmoqlarida	1
144	Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?	2 ta	3 ta	4 ta	kalit ishlatilmaydi	1
145	Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?	1 ta	3 ta	4 ta	kalit ishlatilmaydi	1
146	Kriptotizimlar kalitlar soni bo‘yicha qanday turga bo‘linadi?	simmetrik va assimetrik turlarga	simmetrik va bir kalitli turlarga	3 kalitli turlarga	assimetrik va 2 kalitli turlarga	1
147	Kriptologiya qanday yo‘nalishlarga bo‘linadi?	kriptografiya va kriptotahlil	kriptografiya va kriptotizim	kripto va kriptotahlil	kriptoanaliz va kriptotizim	1
148	Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?	Barcha javoblar to‘g‘ri	Faqat litsenziyali dasturiy ta’minotdan foydalanish.	Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta’minlash va uni doimiy yangilab borish.	Boshqa komyuterda yozib olingan ma’lumotlarni o‘qishdan oldin har bir saqlagichni antivirus tekshiruvidan o‘tkazish.	1
149	Antivirus dasturiy vositalari zararli dasturlarga qarshi to‘liq himoyani ta’minlay olmasligining asosiy sababini ko‘rsating?	Paydo bo‘layotgan zararli dasturiy vositalar sonining ko‘pligi.	Viruslar asosan antivirus ishlab chiqaruvchilar tomonidan yaratilishi.	Antivirus vositalarining samarali emasligi.	Aksariyat antivirus vositalarining pullik ekanligi.	1
150	… umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi.	Tarmoqlararo ekran	Virtual himoyalangan tarmoq	Global tarmoq	Korxona tarmog‘i	1
151	RSA algoritmida p=5, q=13, e=7 ga teng bo‘lsa, shaxsiy kalitni hisoblang?	7	13	65	35	1
152	..... hujumida hujumchi o‘rnatilgan aloqaga suqilib kiradi va aloqani bo‘ladi. Nuqtalar o‘rniga mos javobni qo‘ying.	O‘rtada turgan odam.	Qo‘pol kuch.	Parolga qaratilgan.	DNS izi.	1
153	Agar ob’ektning xavfsizlik darajasi sub’ektning xavfsizlik darajasidan kichik yoki teng bo‘lsa, u holda O‘qish uchun ruxsat beriladi. Ushbu qoida qaysi foydalanishni boshqarish usuliga tegishli.	MAC	DAC	RMAC	ABAC	1
154	GSM tarmog‘ida ovozli so‘zlashuvlarni shifrlash algoritmi bu?	A5/1	DES	ГОСТ	RSA	1
155	RSA algoritmida ochiq kalit e=7, N=35 ga teng bo‘lsa, M=2 ga teng ochiq matnni shifrlash natijasini ko‘rsating?	23	35	5	7	1
156	RSA algoritmida ochiq kalit e=7, N=143 ga teng bo‘lsa, M=2 ga teng ochiq matnni shifrlash natijasini ko‘rsating?	128	49	11	7	1
157	Jumlani to‘ldiring. Agar	jinoyat sifatida	rag‘bat hisoblanadi.	buzg‘unchilik	guruhlar kurashi	1

	axborotning o‘g‘irlanishi moddiy va ma’naviy boyliklarning yo‘qotilishiga olib kelsa.	baholanadi.		hisoblanadi.	hisoblanadi.	
158	Jumlani to‘ldiring. Simli va simsiz tarmoqlar orasidagi asosiy farq ...	tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud mavjudigi.	tarmoq chetki nuqtalari orasidagi xududning kengligi.	himoya vositalarining chegaralanganligi.	himoyani amalga oshirish imkoniyati yo‘qligi.	1
159	Jumlani to‘ldiring. Simmetrik shifrlash algoritmlari ochiq ma’lumotdan foydalanish tartibiga ko‘ra ...	blokli va oqimli turlarga bo‘linadi.	bir kalitli va ikki kalitli turlarga bo‘linadi.	Feystel tarmog‘iga asoslangan va SP tarmog‘iga asoslangan turlarga bo‘linadi.	murakkablikka va tizimni nazariy yondoshuvga asoslangan turlarga bo‘linadi.	1
160	Jumlani to‘ldiring. Tarmoqlararo ekranning vazifasi ...	ishonchli va ishonchsiz tarmoqlar orasida ma’lumotlarga kirishni boshqarish.	tarmoq hujumlarini aniqlash.	trafikni taqiqlash.	tarmoqdagi xabarlar oqimini uzish va ulash.	1
161	Faktorlash muammosi asosida yaratilgan assimetrik shifrlash usuli?	RSA	El-Gamal	Elliptik egri chiziqga asoslangan shifrlash	Diffi-Xelman	1
162	Eng zaif simsiz tarmoq protokolini ko‘rsating?	WEP	WPA	WPA2	WPA3	1
163	Axborotni shifrlashdan maqsadi nima?	Maxfiy xabar mazmunini yashirish.	Ma’lumotlarni zichlashtirish, siqish.	Malumotlarni yig‘ish va sotish.	Ma’lumotlarni uzatish.	1
164	9 soni bilan o‘zaro tub bo‘lgan sonlarni ko‘rsating?	10, 8	6, 10	18, 6	9 dan tashqari barcha sonlar	1
165	12 soni bilan o‘zaro tub bo‘lgan sonlarni ko‘rsating?	11, 13	14, 26	144, 4	12 dan tashqari barcha sonlar	1
166	13 soni bilan o‘zaro tub bo‘lgan sonlarni ko‘rsating?	5, 7	12, 26	14, 39	13 dan tashqari barcha sonlar	1
167	Jumlani to‘ldiring. Autentifikatsiya tizimlari asoslanishiga ko‘ra ... turga bo‘linadi.	3	2	4	5	1
168	… umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi.	Tarmoqlararo ekran	Virtual himoyalangan tarmoq	Global tarmoq	Korxona tarmog‘i	1
169	Antivirus dasturiy vositalari zararli dasturlarga qarshi to‘liq himoyani ta’minlay olmasligining asosiy sababini ko‘rsating?	Paydo bo‘layotgan zararli dasturiy vositalar sonining ko‘pligi.	Viruslar asosan antivirus ishlab chiqaruvchilar tomonidan yaratilishi.	Antivirus vositalarining samarali emasligi.	Aksariyat antivirus vositalarining pullik ekanligi.	1
170	Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?	Barcha javoblar to‘g‘ri	Faqat litsenziyali dasturiy ta’minotdan foydalanish.	Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta’minlash va uni doimiy yangilab borish.	Boshqa komyuterda yozib olingan ma’lumotlarni o‘qishdan oldin har bir saqlagichni antivirus tekshiruvidan o‘tkazish.	1
171	Virus aniq bo‘lganda va xususiyatlari aniq ajratilgan holatda eng katta samaradorlikka ega zararli dasturni aniqlash usulini ko‘rsating?	Signaturaga asoslangan usul	O‘zgarishga asoslangan usul	Anomaliyaga asoslangan usul	Barcha javoblar to‘g‘ri	1
172	Signatura (antiviruslarga aloqador bo‘lgan) bu-?	Fayldan topilgan bitlar qatori.	Fayldagi yoki katalogdagi o‘zgarish.	Normal holatdan tashqari holat.	Zararli dastur turi.	1
173	Zararli dasturiy vositalarga qarshi foydalaniluvchi dasturiy vosita bu?	Antivirus	VPN	Tarmoqlararo ekran	Brandmauer	1
174	Kompyuter viruslarini tarqalish usullarini ko‘rsating?	Ma’lumot saqlovchilari, Internetdan yuklab olish va elektron pochta orqali.	Ma’lumot saqlovchilari, Internetdan yuklab olish va skaner qurilmalari orqali.	Printer qurilmasi, Internetdan yuklab olish va elektron pochta orqali.	Barcha javoblar to‘g‘ri.	1
175	Qurbon kompyuteridagi ma’lumotni shifrlab, uni deshifrlash uchun to‘lovni amalga oshirishni talab	Ransomware.	Mantiqiy bombalar.	Rootkits.	Spyware.	1

	qiluvchi zararli dastur bu-?					
176	Internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bu-?	Botnet.	Backdoors.	Adware.	Virus.	1
177	Biror mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu-?	Mantiqiy bombalar.	Backdoors.	Adware.	Virus.	1
178	Buzg‘unchiga xavfsizlik tizimini aylanib o‘tib tizimga kirish imkonini beruvchi zararli dastur turi bu-?	Backdoors.	Adware.	Virus.	Troyan otlari.	1
179	Ma’lumotni to‘liq qayta tiklash qachon samarali amalga oshiriladi?	Saqlagichda ma’lumot qayta yozilmagan bo‘lsa.	Ma’lumotni o‘chirish Delete buyrug‘i bilan amalga oshirilgan bo‘lsa.	Ma’lumotni o‘chirish Shifr+Delete buyrug‘i bilan amalga oshirilgan bo‘lsa.	Formatlash asosida ma’lumot o‘chirilgan bo‘lsa.	1
180	Ma’lumotni zaxira nusxalash nima uchun potensial tahdidlarni paydo bo‘lish ehtimolini oshiradi.	Tahdidchi uchun nishon ko‘payadi.	Saqlanuvchi ma’lumot hajmi ortadi.	Ma’lumotni butunligi ta’minlanadi.	Ma’lumot yo‘qolgan taqdirda ham tiklash imkoniyati mavjud bo‘ladi.	1
181	Qaysi xususiyatlar RAID texnologiyasiga xos emas?	Shaxsiy kompyuterda foydalanish mumkin.	Serverlarda foydalanish mumkin.	Xatoliklarni nazoratlash mumkin.	Disklarni “qaynoq almashtirish” mumkin.	1
182	Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo‘shimcha apparat va dasturiy vositani talab qiladi?	Lentali disklar.	Ko‘chma qattiq disklar.	USB disklar.	CD/DVD disklar.	1
183	Ma’lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi?	Zarur axborotni tanlashdan.	Mos zaxira nusxalash vositasini tanlashdan.	Mos zaxira nusxalash usulini tanlashdan.	Mos RAID sathini tanlashdan.	1
184	Jumlani to‘ldiring. .... - muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi.	Ma’lumotlarni zaxira nusxalash	Kriptografik himoya	VPN	Tarmoqlararo ekran	1
185	Paket filteri turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi?	Tarmoq sathi parametrlari asosida.	Kanal sathi parametrlari asosida.	Ilova sathi parametrlari asosida.	Taqdimot sathi parametrlari asosida.	1
186	Jumlani to‘ldiring. ... texnologiyasi lokal simsiz tarmoqlarga tegishli.	WI-FI	WI-MAX	GSM	Bluetooth	1
187	Jumlani to‘ldiring. Kriptografik himoya axborotning ... xususiyatini ta’minlamaydi.	Foydalanuvchanlik	Butunlik	Maxfiylik	Autentifikatsiya	1
188	Jumlani to‘ldiring. Parol kalitdan .... farq qiladi.	tasodifiylik darajasi bilan	uzunligi bilan	belgilari bilan	samaradorligi bilan	1
189	Parolga “tuz”ni qo‘shib xeshlashdan maqsad?	Tahdidchi ishini oshirish.	Murakkab parol hosil qilish.	Murakkab xesh qiymat hosil qilish.	Ya’na bir maxfiy parametr kiritish.	1
190	Axborotni foydalanuvchanligini buzishga qaratilgan tahdidlar bu?	DDOS tahdidlar.	Nusxalash tahdidlari.	Modifikatsiyalash tahdidlari.	O‘rtaga turgan odam tahdidi.	1
191	Tasodifiy tahdidlarni ko‘rsating?	Texnik vositalarning buzilishi va ishlamasligi.	Axborotdan ruxsatsiz foydalanish.	Zararkunanda dasturlar.	An’anaviy josuslik va diversiya.	1
192	Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga imkon beruvchi himoya vositasi bu?	Tarmoqlararo ekran.	Virtual Private Network.	Antivirus.	Router.	1
193	Qaysi himoya vositasi yetkazilgan axborotning butunligini tekshiradi?	Virtual Private Network.	Tarmoqlararo ekran.	Antivirus.	Router.	1
194	Qaysi himoya vositasi tomonlarni	Virtual Private Network.	Tarmoqlararo ekran.	Antivirus.	Router.	1

	autentifikatsiyalash imkoniyatini beradi?					
195	Foydalanuvchi tomonidan kiritilgan taqiqlangan so‘rovni qaysi himoya vositasi yordamida nazoratlash mumkin.	Tarmoqlararo ekran.	Virtual Private Network.	Antivirus.	Router.	1
196	Qaysi himoya vositasi mavjud IP - paketni to‘liq shifrlab, unga yangi IP sarlavha beradi?	Virtual Private Network.	Tarmoqlararo ekran.	Antivirus.	Router.	1
197	Ochiq tarmoq yordamida himoyalangan tarmoqni qurish imkoniyatiga ega himoya vositasi bu?	Virtual Private Network.	Tapmoklapapo ekran.	Antivirus.	Router.	1
198	Qaysi himoya vositasida mavjud paket shifrlangan holda yangi hosil qilingan mantiqiy paket ichiga kiritiladi?	Virtual Private Network.	Tarmoqlararo ekran.	Antivirus.	Router.	1
199	Qaysi himoya vositasi tarmoqda uzatilayotgan axborotni butunligi, maxfiyligi va tomonlar autentifikatsiyasini ta’minlaydi?	Virtual Private Network.	Tarmoqlararo ekran.	Antivirus.	Router.	1
200	Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi.	Tarmoqlararo ekran.	Antivirus.	Virtual himoyalangan tarmoq.	Router.	1

Akademik faoliyatni boshqarish bo’limi: I. Aripov

Axborot texnologiyalari fakulteti dekani: B.E.To‘rayev

“Komputer injiniringi” kafedrasi mudiri: R.Meliqo’ziyev