1. Axborot xavfsizligining asosiy maqsadlaridan biri-bu…

Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish

2. Windows OTda necha turdagi hodisa ro‘yxatga olinadi?

a) 5 ta

3. Konfidentsiallikga to‘g‘ri ta’rif keltiring.

a) axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

4. Kriptografiya faninining asosiy maqsadi nima?

a) maxfiylik, yaxlitlilikni ta’minlash

5. Kriptografiyada kalitning vazifasi nima?

b) Matnni shifrlash va shifrini ochish uchun kerakli axborot

6. Qo‘yish, o‘rin almashtirish, gammalash kriptografiyaning qaysi turiga bog‘liq?

a) simmetrik kriptotizimlar

7. Autentifikatsiya nima?

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

8. Identifikatsiya bu- …

a) Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni

9. Kriptobardoshlilik deb nimaga aytilladi?

a) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

10. Kriptografiyada matn –bu..

a) alifbo elementlarining tartiblangan to‘plami

11. Kriptotizimga qo‘yiladigan umumiy talablardan biri nima?

a) shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak

12. Berilgan ta’riflardan qaysi biri assimetrikrik tizimlarga xos?

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

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

a) login

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

a) parol

15. Ro‘yxatdan o‘tish-bu…

a) foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni

16. Axborot qanday sifatlarga ega bo‘lishi kerak?

a) ishonchli, qimmatli va to‘liq

17. Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish nima deb ataladi?

b) steganografiya

18. Kriptografiya fan sifatida shakllanishida nechta davrlarga bo‘linadi?

a) 4 ga

19. Shifrmatntni ochiq matntga akslantirish jarayoni nima deb ataladi?

a) Deshifrlash

20. Risk-tushunchasi nima?

a) Belgilangan sharoitda tahdidning manbalarga bo‘lishi mumkin bo‘lgan zarar yetkazilishini kutish

21. Tahdid-tushunchasi nima?

a) Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa

22. Kodlash terminiga berilgan ta’rifni belgilang.

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

23. Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug‘ullanadi?

b) Kriptoanaliz

24. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?

a) {d, n} – yopiq, {e, n} – ochiq;

25. Zamonaviy kriptografiya qanday bo‘limlardan iborat?

a) Simmetrik kriptotizimlar; Ochiq kalitli kriptotizimlar; Elektron raqamli imzo; Kalitlarni boshqarish

26. Shifr nima?

a) Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo‘lgan krptografik algoritm

27. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

b) Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

28. Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?

c) Xesh funksiyalar

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

a) Avtorizatsiya

30. Autentifikatsiya faktorlari nechta?

b) 3 ta

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

a) Biometrik autentifikatsiya

32. Shifrlash kaliti noma’lum bo‘lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini belgilaydigan atamani toping.

b) Kriptobardoshlik

33. Qog‘oz ma’lumotlarni yo‘q qilish odatda necha xil usuldan foydalaniladi?

a) 4 xil

34. Kiberjinoyat qanday turlarga bo‘linadi?

a) Ichki va tashqi

35. “Kiberxavfsizlik to‘g‘risida” Qonun qachon tasdiqlangan?

a) 15.04.2022 y

36. Kiberjinoyatchilik bu –. . .

a) Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.

37. Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?

d) Texnik vositalarning buzilishi va ishlamasligi

38. Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?

c) Ma’lumotlar butunligi

39. Biometrik autentifikatsiyalashning avfzalliklari-bu:

b) Biometrik parametrlarning noyobligi

40. Simmetrik shifrlashning noqulayligi – bu:

a) Maxfiy kalitlar bilan ayirboshlash zaruriyatidir

41. Token, smartkartalarda xavfsizlik tomonidan kamchiligi nimada?

a) Foydalanish davrida maxfiylik kamayib boradi

b) Qurilmalarni ishlab chiqarish murakkab jarayon

**c) Qurilmani yo‘qotilishi katta xavf olib kelishi mumkin**

d) Qurilmani qalbakilashtirish oson

42. Ma’lumotlarni yo‘qolish sabab bo‘luvchi tabiiy tahdidlarni ko‘rsating

a) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

**b) Zilzila, yong‘in, suv toshqini va hak.**

c) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi

d) Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani

43. Ma’lumotlarni tasodifiy sabablar tufayli yo‘qolish sababini belgilang

**a) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi**

b) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi

c) Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

d) Zilzila, yong‘in, suv toshqini va hak.

44. Ma’lumotlarni inson xatosi tufayli yo‘qolish sababini belgilang.

a) Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi.

**b) Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.**

c) Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi

d) Zilzila, yong‘in, suv toshqini va hak.

45. "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?

a) Parolni esda saqlash kerak bo‘ladi.

b) Parolni almashtirish jarayoni murakkabligi

c) Parol uzunligi soni cheklangan

**d) Foydalanish davrida maxfiylik kamayib boradi**

46. Nima uchun autentifikatsiyalashda parol ko‘p qo‘llaniladi?

**a) Sarf xarajati kam, almashtirish oson**

b) Parolni foydalanubchi ishlab chiqadi

c) Parolni o‘g‘rishlash qiyin

d) Serverda parollar saqlanmaydi

47. Elektron xujjatlarni yo‘q qilish usullari qaysilar?

a) Yoqish, ko‘mish, yanchish

**b) Shredirlash, magnitsizlantirish, yanchish**

c) Shredirlash, yoqish, ko‘mish

d) Kimyoviy usul, yoqish.

48. Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?

a) 4 taga

b) 2 taga

c) 5 taga

**d) 3 taga**

49. Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi?

**a) Knx1@8&h**

b) qwertyu

c) salomDunyo

d) Mashina505

50. Parollash siyosatiga ko‘ra parol tanlash shartlari qanday?

a) Kamida 7 belgi; katta va kichik xavflar, sonlar qo‘llanishi kerak.

**b) Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo‘llanishi kerak.**

c) Kamida 6 belgi; katta xarflar, sonlar , kamida bitta maxsus simvol qo‘llanishi kerak.

d) Kamida 6 belgi; katta va kichik xarflar, kamida bitta maxsus simvol qo‘llanishi kerak.

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

a) Kodlash

**b) Xeshlash**

c) Shifrlash

d) Stenografiya

52. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to‘g‘ri keladi?

a) O‘rta asr davrida

b) 15 asr davrida

**c) 1-2 jahon urushu davri**

d) 21 asr davrida

53. "Fishing" tushunchasi-bu…:

a) Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

b) Kompyuter, dasturlar va tarmoqlar xavfsizligi

**c) Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan internet-hujumi**

d) Kompyuter tizimlariga ruxsatsiz ta’sir ko‘rsatish

54. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so‘zi nimani anglatadi?

a) Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko‘rsatmalar, amaliyot.

b) Hisoblash tizimi xizmatlaridan foydalanish huqu kiberxavfsizlik qiga ega shaxs (shaxslar guruxi, tashkilot).

**c) Axborot xavfsizligida tashkilot uchun qimmatbaho bo‘lgan va himoyalanishi lozim bo‘lgan narsalar**

d) Ma’lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo‘ljallangan dasturiy va apparat vositalar

55. Axborot xavfsizligi timsollarini ko‘rsating.

a) Haker, Krakker

**b) Alisa, Bob, Eva**

c) Buzg‘unchi, hujumchi

d) subyekt, user

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

**a) Qonunlar**

b) Qarorlar

c) Standartlar

d) Farmonlar

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

a) Ruxsat berishga asoslangan siyosat

b) Paranoid siyosat

c) Extiyotkorlik siyosati

**d) Nomuntazam siyosat**

58. “Hаmmа nаrsа tа’qiqlаnаdi.” Bu qаysi xаvfsizlik siyosаtigа xos?

a) Ruxsаt berishgа аsoslаngаn siyosаt (Permissive Policy)

**b) Pаrаnoid siyosаti (Pаrаnoid Policy)**

c) Ehtiyotkorlik siyosаti (Prudent Policy)

d) Nomuntаzаm siyosаt (Promiscuous Policy

59. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…

a) Kibersport deb ataladi

b) Kiberterror deb ataladi

**c) Kiberjinoyat deb ataladi**

d) Hakerlar uyushmasi deyiladi

60. Qaysi siyosat turli hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi?

**a) Maqbul foydalanish siyosati**

b) Paranoid siyosat

c) Ruxsat berishga asoslangan siyosat

d) Nomuntazam siyosat

61. Qaysi siyosatda Adminstrator xavfsiz va zarur xizmatlarga indvidual ravishda ruxsat beradi?

a) Paranoid siyosat

b) Ruxsat berishga asoslangan siyosat

c) Nomuntazam siyosat

**d) Extiyotkorlik siyosati**

62. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?

a) Nomuntazam siyosat

b) Paranoid siyosat

**c) Ruxsat berishga asoslangan siyosat**

d) Extiyotkorlik siyosati

63. Qaysi siyosatga ko‘ra hamma narsa taqiqlanadi?

a) Ruxsat berishga asoslangan siyosat

b) Nomuntazam siyosat

c) Extiyotkorlik siyosati

**d) Paranoid siyosat**

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

**a) Xavfsizlik siyosat**

b) Standart

c) Qaror

d) Buyruq

65. Xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to‘liq tasavvurga ega shaxs kim deb ataladi?

a) Xavfsizlik mutaxasisi

b) Rahbar

c) Foydalanuvchi

**d) Xavfsizlik ma'muri (admin)**

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

**a) Xalqaro va milliy huquqiy me’yorlarni**

b) Tashkiliy va xalqaro me’yorlarni

c) Ananaviy va korporativ me’yorlarni

d) Davlat va nodavlat tashkilotlari me’yorlarni

67. Ehtiyotkorlik siyosati (Prudent Policy) – bu ….

a) Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi

b) Hamma narsa ta’qiqlanadi

c) Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi

**d) Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi**

68. ... - faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot.

**a) Parol**

b) Login

c) Maxfiy kalit

d) Shifrlangan axborot

69. “Dasturiy ta’minotlar xavfsizligi” bilim sohasi - bu ...

**a) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.**

**b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.**

c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

d) 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.

70. “Jamoat xavfsizligi” bilim sohasi - bu …

**a) u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi.**

b) tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini

c) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi

d) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

71. “Ma’lumotlar xavfsizligi” bilim sohasi - bu …

**a) ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.**

b) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi

c) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

d) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

72. “Tizim xavfsizligi” bilim sohasi - bu …

**a) tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi.**

b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

d) 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.

73. “Xodim xavfsizligi” tushunchasi- bu…

**a) Qandaydir jiddiy axborotdan foydalanish imkoniyatiga ega barcha xodimlarning kerakli avtorizatsiyaga va barcha kerakli ruxsatnomalarga egalik kafolatini ta’minlovchi usul.**

b) Axborot tarmog‘ini ruxsatsiz foydalanishdan, me’yoriy harakatiga tasodifan aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.

c) Destruktiv harakatlarga va yolg‘on axborotni zo‘rlab qabul qilinishiga olib keluvchi ishlanadigan va saqlanuvchi axborotdan ruxsatsiz foydalanishga urinishlarga kompyuter tizimining qarshi tura olish hususiyati.

d) Korxona o‘z faoliyatini buzilishsiz va to‘xtalishsiz yurgiza oladigan vaqt bo‘yicha barqaror bashoratlanuvchi atrof-muhit holati.

74. “Yaxlitlik” atamasiga berilgan ta’rifni belgilang.

**a) Bu yozilgan va xabar qilingan ma’luotlarning haqiqiyligini, to‘g‘riligini, butunligini saqlash qobiliyati**

b) Funksionala imkoniyatni o‘z vaqtida foydalanish

c) Tizimning ruxsat berilgan foydalanish uchun ma’lumot tarqatishni cheklash

d) Korxona o‘z faoliyatini buzilishsiz va to‘xtalishsiz yurgiza oladigan vaqt bo‘yicha barqaror bashoratlanuvchi atrof-muhit holati

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

**a) Kiberxavfsizlik**

b) Axborot xavfsizligi

c) Kiberjtnoyatchilik

d) Risklar

76. Assimetrikrik kriptotizimlarda axborotni shifrlashda va deshifrlash uchun qanday kalit ishlatiladi?

**a) Ikkita kalit: ochiq va yopiq**

b) Bitta kalit

c) Elektron raqamli imzo

d) Foydalanuvchi identifikatori

77. Autentifikatsiya jarayoni qanday jarayon?

**a) obyekt yoki subyektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy axborotni tekshirish orqali asilligini aniqlash**

b) axborot tizimlari obyekt va subyektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo‘yicha solishtirib uni aniqlash jarayoni

c) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

d) foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni

78. Avtorizatsiya nima?

a) Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilarga tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni

b) Subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim qilish jarayoni

c) Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni

d) Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilar

79. Axborot o‘lchovini kamayish tartibini to‘g‘ri tanlang

a) Terabayt,gigabayt,megabayt

b) Bit,bayt,kilobayt,megabayt

c) Gigabayt,megabayt,bayt

d) Gigabayt,megabayat,terobayt

80. Axborot o‘lchovini o‘sish tartibini to‘g‘ri tanlang

a) Kilobayt,megabayt,gigabayt

b) Bit,bayt,megabayt,kilobayt

c) Gigabayt,megabayt,pikobayt

d) Gigabayt,terabayt,pikobayt

81. Axborot xavfsizligi qanday asosiy xarakteristikalarga ega?

a) Butunlik, konfidentsiallik, foydalanuvchanlik

b) Butunlik, himoya, ishonchlilikni o‘rganib chiqishlilik

c) Konfidentsiallik, foydalana olishlik

d) Himoyalanganlik, ishonchlilik, butunlik

82. Axborot xavfsizligining huquqiy ta'minotiga nimalar kiradi?

a) Qonunlar, aktlar, me'yoriy-huquqiy hujjatlar, qoidalar, yo‘riqnomalar, qo‘llanmalar majmui

b) Qoidalar yo‘riqnomalar, tizim arxetikturasi, xodimlar malakasi, yangi qoidalar, yangi yo‘riqnomalar, qo‘llanmalar majmui

c) Qoidalar, yo‘riqnomalar, tizim strukturasi, dasturiy ta’minot

d) Himoya tizimini loyihalash, nazorat usullari

83. "Barcha xizmatlar blokirovka qilingandan so‘ng bog‘lanadi". -Bu qaysi xavfsizlik siyosatiga hos?

a) Ehtiyotkorlik siyosati (Prudent Policy)

b) Nomuntazam siyosat (Promiscuous Policy)

c) Paranoid siyosati (Paranoid Policy)

d) Ruxsat berishga asoslangan siyosat (Permissive Policy)

84. Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo‘linadi?

a) Blokli va oqimli

b) DES va oqimli

c) Feystel va Verman

d) SP− tarmoq va IP

85. BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?

a) AES, Serpent, Twofish

b) Pleyfer, Sezar

c) DES, sezar, Futurama

d) AES, Serpent, Twofish, Triple DES, GOST 28147-89

86. Blokli shifrlash tushunchasi nima?

a) shifrlanadigan matn blokiga qo‘llaniladigan asosiy akslantirish

b) murakkab bo‘lmagan kriptografik akslantirish

c) axborot simvollarini boshqa alfavit simvollari bilan almashtirish

d) ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi

87. Elektron pochtaga kirishda foydalanuvchi qanday autetntifikasiyalashdan o‘tadi?

a) Parol asosida

b) Smart karta asosida

c) Biometrik asosida

d) Ikki tomonlama

88. Elektron raqamli imzo - bu …

a) xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimcha

b) matnni shifrlash va shifrini ochish uchun kerakli axborot

c) axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam

d) kalit axborotni shifrlovchi kalitlar

89. Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?

a) Imzo qo‘yish va imzoni tekshirishdan

b) Faqat imzo qo‘yishdan

c) Faqat imzoni tekshirishdan

d) Kalitlarni taqsimlashdan

90. Elektron raqamli imzo kalitlari ro‘yxatga olish qaysi tashkilot tomonidan bajariladi

a) Sertifikatlari roʻyxatga olish markazlari

b) Tegishli Vazirliklar

c) Axborot xavfsizligi markazlari

d) Davlat Hokimiyati

91. Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima?

a) Autentifikatsiya

b) Identifikatsiya

c) Avtorizatsiya

d) Ma’murlash

92. Kriptografiyada kalit – bu …

a) Matnni shifrlash va shifrini ochish uchun kerakli axborot

b) Bir qancha kalitlar yig‘indisi

c) Axborotli kalitlar to‘plami

d) Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

93. Kiberetika tushunchasi-bu…

a) Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

b) Kompyuter, dasturlar va tarmoqlar xavfsizligi

c) Kompyuter tizimlariga ruxsatsiz ta’sir ko‘rsatish

d) Tashkilot va odamlarning mahsus va shahsiy ma’lumotlarini olishka qaratilgan internet-atakasi

94. Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi?

a) tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi

b) tashkilot xodimlari himoyasini ta’minlaydi

c) tashkilot axborotlari va binolarining himoyasini ta’minlaydi

d) tashkilot omborini va axborotlari himoyasini ta’minlaydi

95. Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda qo‘llaniladi?

a) ochiq kalitlar

b) yopiq kalitlar

c) seans kalitlari

d) Barcha tutdagi kalitlar

96. Kriptografiyada "alifbo" deganda nima tushuniladi?

a) axborotni ifodalashda ishlatiluvchi bilgilarning chekli to‘plami tushuniladi

b) matnni shifrlash va shifrini ochish uchun kerakli axborot

c) xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimcha

d) alfavit elementlaridan tartiblangan nabor

97. O‘zbekistonda masofadan elektron raqamli imzo olish uchun qaysi internet manzilga murojaat qilinadi?

a) e-imzo.uz

b) elektron-imzo.uz

c) imzo.uz

d) eri.uz

98. Oqimli shifrlashning mohiyati nimada?

a) Oqimli shifrlash birinchi navbatda axborotni bloklarga bo‘lishning imkoni bo‘lmagan hollarda zarur,

b) Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo‘natish uchun oqimli shifrlash zarur,

c) Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo‘yicha shifrlaydi

d) Oqimli shifrlash birinchi navbatda axborotni bloklarga bo‘lishning imkoni bo‘lgan hollarda zarur,

99. RSA algoritmi qanday jarayonlardan tashkil topgan?

a) Kalitni generatsiyalash; Shifrlash; Deshifrlash.

b) Shifrlash; Imzoni tekshirish; Deshifrlash

c) Kalitni generatsiyalash; imzolash; Deshifrlash.

d) Imzoni tekshirish ; Shifrlash; Deshifrlash.

100. 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?

a) login

b) parol

c) identifikatsiya

d) maxfiy maydon

101. Shifrlash qanday jarayon?

a) akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi

b) kalit asosida shifrmatn ochiq matnga akslantiriladi

c) shifrlashga teskari jarayon

d) almashtirish jarayoni bo‘lib: ochiq matn deb nomlanadigan matn o‘girilgan holatga almashtiriladi

102. Kichik xajmdagi xotira va hisoblash imkoniyatiga ega bo‘lgan, o‘zida parol yoki kalitni saqlovchi qurilma nima deb ataladi?

a) Token, Smartkarta

b) Chip

c) Fleshka

d) Disk

103. Cisco tashkiloti “kiberxavfsizlik” atamasiga qanday ta’rif bergan?

a) Kiberxavfsizlik - tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti

b) Hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan

c) Bu yozilgan va xabar qilingan ma’luotlarning haqiqiyligini, to‘g‘riligini, butunligini saqlash qobiliyati

d) Ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.

104. Foydalanuvchanlik-bu…

a) avtorizatsiyalangan mantiqiy obyekt so‘rovi bo‘yicha axborotning tayyorlik va foydalanuvchanlik holatida bo‘lishi xususiyati

b) axborotning buzilmagan ko‘rinishida (axborotning qandaydir qayd etilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati

c) axborot yoki uni eltuvchisining shunday holatiki, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi

d) potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi

105. Kiberxavfsizlik bilim sohasi nechta bilim sohasini o‘z ichiga oladi?

a) 8 ta

b) 7 ta

c) 6 ta

d) 5 ta

106. Ijtimoiy (sotsial) injineriya-bu…

a) turli psixologik usullar va firibgarlik amaliyotining to‘plami, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olish

b) Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish

c) axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi

d) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

107. Kiberxavfsizlik arxitekturasi nechta sathga ajratiladi?

a) 3ta

b) 2 ta

c) 4 ta

d) 5 ta

108. Tashkilot axborot xavfsizligi siyosati-bu…

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.

b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.

c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.

d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

109. Muammoga qaratilgan xavfsizlik siyosatlari …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.

**b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.**

c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.

d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

110. Tizimga qaratilgan xavfsizlik siyosatlari …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.

b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.

**c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.**

d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.

111. Internetdan foydalanish siyosati. …

a) mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi.

b) bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.

c) mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi.

**d) mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi.**

112. Ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o‘zgartirishlar oilasi-…

**a) Kriptotizim**

b) Deshifrlash

c) Rasshifrovkalash

d) Shifrlash

113. O‘zgartirishlar oilasidan birini tanlashni ta’minlovchi kriptografik algoritmning qandaydir parametrlarining muayyan qiymati-…

a) Kriptotizim

**b) Kalit**

c) Rasshifrovkalash

d) Shifrlash

114. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuning maqsadi nimadan iborat?

a) Har kimning axborotni erkin va moneliksiz izlash, olish, tadqiq etish, uzatish hamda tarqatishga doir konstitutsiyaviy huquqini amalga oshirish jarayonida yuzaga keladigan munosabatlarni tartibga solish

b) Axborotlarni maxfiylashtirish va maxfiylikdan chiqarish ushbu Qonunga hamda o‘zbekiston Respublikasi Vazirlar Mahkamasi tasdiqlaydigan ma’lumotlarning maxfiylik darajasini aniqlash va belgilash

c) Shaxsga doir ma’lumotlar sohasidagi munosabatlarni tartibga solish.

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

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

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

b) Shaxsga doir ma’lumotlar sohasidagi munosabatlarni tartibga solish.

c) Har kimning axborotni erkin va moneliksiz izlash, olish, tadqiq etish, uzatish hamda tarqatishga doir konstitutsiyaviy huquqini amalga oshirish jarayonida yuzaga keladigan munosabatlarni tartibga solish

d) Axborotlarni maxfiylashtirish va maxfiylikdan chiqarish ushbu Qonunga hamda o‘zbekiston Respublikasi Vazirlar Mahkamasi tasdiqlaydigan ma’lumotlarning maxfiylik darajasini aniqlash va belgilash

116. "Backdoors"-qanday zararli dastur?

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

b) foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod

c) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi

d) marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot

117. .... – o‘zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma’lumoti va xavfsizlik algoritmlarini saqlaydi.

a) Sim karta

b) Token

c) Smart karta

d) Elektron raqamli imzo

118. .... kompyuter tarmoqlari bo‘yicha tarqalib, kompyuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o‘zining nusxasini qoldiradi.

a) “Chuvalchang” va replikatorli virus

b) Kvazivirus va troyan virus

c) Troyan dasturi

d) Mantiqiy bomba

119. “Aloqa xavfsizligi” bilim sohasi - bu …

a) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi.

c) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.

d) 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.

120. “Avtorizatsiya” atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

a) Foydalanishni boshqarish

b) Tarmoqni loyihalash

c) Foydalanish

d) Identifikatsiya

121. “Inson xavfsizligi” bilim sohasi - bu …

a) 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

b) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi

c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

d) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi

122. “Tashkil etuvchilar xavfsizligi” - bu …

a) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi

b) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi

c) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi

d) 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

123. “Tashkilot xavfsizligi” bilim sohasi - bu …

a) tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini

b) foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi

c) katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi

d) tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi

124. …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.

a) UDP

b) HTTP

c) TCP

d) FTP

125. ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.

a) TCP

b) IP

c) HTTP

d) FTP

126. Access control list va Capability list bu nimaning asosiy elementi hisoblanadi?

a) Lampson matritsasining

b) XASML standartining

c) Role-based access control RBACning

d) Attribute based access control (ABAC)ning

127. “Adware” zararli dastur xususiyati nimadan iborat?

a) marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.

b) foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.

c) bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi.

d) o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi

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

a) "Issiq zaxiralash"

b) "Sovuq saxiralash"

c) "Iliq saxiralash"

d) "To‘liq zaxiralash"

129. Qaysi zaxiralash usuli offlayn zaxiralash deb ham atalib, tizim ishlamay turganida yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi?

a) "Sovuq saxiralash"

b) "Issiq zaxiralash"

c) "Iliq saxiralash"

d) "To‘liq zaxiralash"

130. Qaysi zaxiralashda tizim muntazam yangilanishni amalga oshirish uchun tarmoqqa bog‘lanishi kerak bo‘ladi?

a) "Iliq saxiralash"

b) "Sovuq saxiralash"

c) "Issiq zaxiralash"

d) "To‘liq zaxiralash"

131. Agar RSA algotirmida e-ochiq kalitni, d-maxfiy kalitni, n-modul ifodalasa, qaysi formula deshifrlashni ifodalaydi?

a) M = C^d mod n;

b) C = M^d mod n;

c) C = M^ed mod n;

d) M = C^e mod n;

132. Agar RSA algotirmida e-ochiq kalitni, d-maxfiy kalitni, n-modul , qaysi formula shifrlashni ifodalaydi?

a) C = M^e mod n;

b) C = M^d mod n;

c) C = M^ed mod n;

d) M = C^e mod n;

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

a) Tamoqlararo ekranlarning o‘rnatilishi

b) Tashkiliy ishlarni bajarilishi

c) Globol tarmoqdan uzib qo‘yish

d) Aloqa kanallarida optik toladan foydalanish

134. Akslantirish tushunchasi deb nimaga aytiladi?

a) 1-to‘plamli elementlariga 2-to‘plam elementalriga mos bo‘lishiga

b) 1-to‘plamli elementlariga 2-to‘plam elementalrini qarama-qarshiligiga

c) har bir elementni o‘ziga ko‘payimasiga

d) agar birinchi va ikinchi to‘plam bir qiymatga ega bo‘lmasa

135. Antivirus dasturiy vositalari viruslarni tahlil qilishiga ko‘ra necha turga bo‘linadi?

a) 2 turga fayl signaturaga va tahlilga asoslangan

b) 2 turga faol va passiv

c) 2 turga pulli va pulsiz

d) 2 turga litsenziyali va ochiq

136. Antivirus dasturlarini ko‘rsating.

a) Drweb, Nod32, Kaspersky

b) arj, rar, pkzip, pkunzip

c) winrar, winzip, winarj

d) pak, lha

137. Antiviruslar viruslarni asosan qanday usulda aniqlaydi?

a) Signaturaga asoslangan

b) Anomaliyaga asoslangan

c) O‘zgarishni aniqlashga asoslangan

d) Defragmentatsiya qilish

138. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud.

a) detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar

b) detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar

c) vaktsinalar, privivkalar, revizorlar, matnhiruvchilar

d) privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar

139. AQShning axborotni shifrlash standartini keltirilgan javobni ko‘rsating?

a) DES(Data Encryption Standart)

b) RSA (Rivest, Shamir ва Adleman)

c) AES (Advanced Encryption Standart)

d) Aniq standart ishlatilmaydi

140. Assimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?

a) shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun

b) shifrlash, deshifrlash, kalit generatsiyalash

c) ERI hosil qilsih, maxfiylikni ta’minlash, kalitlar almashish uchun

d) shifrlash, deshifrlash, kalitlar boshqarish uchun

141. Assimmetrik kriptotizimlarda axborotni shifrlashda va deshifrlash uchun nechta kalit ishlatiladi?

a) Ikkita kalit

b) Bitta kalit

c) Uchta kalit

d) Foydalanuvchi identifikatori

142. Asosan tarmoq, tizim va tashkilot haqidagi axborotni olish maqasadida amalga oshiriladigan tarmoq hujumini belgilang.

a) Razvedka hujumlari

b) Kirish hujumlari

c) DOS hujumi

d) Zararli hujumlar

143. Atribute based access control ABAC usuli attributlari qaysilar?

a) Foydalanuvchi attributlari

b) Asosiy va qo‘shimcha atributlar

c) Tizim attributlari, server atributlari

d) Ichki va tashqi attributlar

144. Autentifikatsiyaga ta'rif qaysi javobda keltirilgan?

a) Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi

b) Tizim meyoriy va g‘ayritabiiy hollarda rejalashtirilgandek o‘zini tutishligi holati

c) Istalgan vaqtda dastur majmuasining mumkinligini kafolati

d) Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi

145. Avtorizatsiya qanday jarayon?

a) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

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

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

d) foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni

146. Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?

a) Korporativ va umumfoydalanuvchi

b) Regional, korporativ

c) Lokal, global

d) Shaharlararo, lokal, global

147. Axborot paketlarini qachon ushlab qolish mumkin?

a) Aloqa kanallari orqali uzatishda

b) Xotira qurilmalarida saqlanayotganda

c) Kompyuter ishga tushganda

d) Ma’lumotlar nusxalanayotganda

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

a) Axborot resursi

b) Axborot xavfsizligi

c) Ma'lumotlar bazasi

d) Axborot tizimlari

149. Axborot tizimiga ta’rif bering.

a) Qo‘yilgan maqsadga erishish yo‘lida axborotlarni olish, qayta ishlash, va uzatish uchun usullar, vositalar va xodimlar jamlanmasi

b) Material olamda axborot almashinuvining yuzaga kelishini ta’minlovchi axborot uzatuvchi, aloqa kanallari, qabul qilgich vositalar jamlanmasi

c) Qo‘yilgan maqsadga erishish yo‘lida o‘zaro birlashtirilgan va ayni vaqtda yagona deb qaraluvchi elementlar to‘plami

d) Ishlab chiqarish jarayonida insonlarning umumiy munosabatlarini ifodalovchi vositlar to‘plami

150. Axborot xavfsizligi siyoatining necha xil turi bor?

a) 3

b) 4

c) 5

d) 2

151. Axborot xavfsizligi siyosati –bu …

a) tashkilot o‘z faoliyatida rioya qiladigan axborot xavfsizligi sohasidagi hujjatlangan qoidalar, muolajalar, amaliy usullar yoki amal qilinadigan prinsiplar majmui sanalib, u asosida tashkilotda axborot xavfsizligi ta’minlanadi

b) mavjud tahdidni amalga oshirilgan ko‘rinishi bo‘lib, bunda kutilgan tahdid amalga oshiriladi

c) mavjud bo‘lgan zaiflik natijasida bo‘lishi mumkin bo‘lgan hujum turi bo‘lib, ular asosan tizimni kamchiliklarini o‘rganish natijasida kelib chiqadi

d) tizimda mavjud bo‘lgan xavfsizlik muammoasi bo‘lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

152. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

a) Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan

b) Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhumligi bilan

c) Axborotni noqonuniy foydalanishlardan o‘zgartirishlardan va yo‘q qilishlardan himoyalanganligi bilan

d) Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bilan

153. Axborot xavfsizligini ta'minlovchi choralarni ko‘rsating?

a) 1-huquqiy, 2-tashkiliy-ma'muriy, 3-dasturiy-texnik

b) 1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy

c) 1-amaliy, 2-tashkiliy-ma'muriy, 3-huquqiy

d) 1-apparat, 2-texnikaviy, 3-huquqiy

154. Axborotdan oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan?

a) AQSH sog‘liqni saqlash va insonlarga xizmat ko‘rsatish vazirligi

b) AQSH Mudofaa vazirligi

c) O‘zbekiston Axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi

d) Rossiya kiberjinoyatlarga qarshu kurashish davlat qo‘mitasi

155. Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?

a) USB fleshka, CD va DVD disklar

b) Qattiq disklar va CDROM

c) CD va DVD, kesh xotira

d) Qattiq disklar va DVDROM

156. Axborotni himoyalash uchun ... usullari qo‘llaniladi.

a) kodlashtirish, kriptografiya, stegonografiya

b) shifrlash va kriptografiya, maxsus yozilgan kod

c) Stegonografiya, kriptografiya, orfografiya

d) Kriptoanaliz, kodlashtirish, zahiralash

157. Axborotning buzilishi yoki yo‘qotilishi xavfiga olib keluvchi himoyalanuvchi obyektga qarshi qilingan xarakatlar qanday nomlanadi?

a) Tahdid

b) Zaiflik

c) Hujum

d) Butunlik

158. Axborotning eng kichik o‘lchov birligi nima?

a) bit

b) kilobayt

c) bayt

d) kilobit

159. Axbоrоt tizimlari xavfsizligining auditi-bu…

a) Axborot tizimlarining himoyalanishining joriy holati, tizim haqida obyektiv ma’lumotlarni olish va baholash

b) Ma`lumоtlarini tahlillash va chоra ko‘rishni tizim haqida subyektiv ma’lumotlarni olish va baholashni tahlil qiladi

c) Ma`lumоtlarini tarqatish va boshqarish

d) Axbоrоtni yig‘ish va korxona tarmog‘ini tahlillash

160. TrueCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?

a) AES, Serpent va Twofish

b) Serpent, RSA

c) El-Gamal, Twofish

d) DES

161. "Bag" atamasini nima ma'noni beradi?

a) Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo

b) Mualliflik huquqini buzilishi

c) Dasturlardagi ortiqcha reklamalar

d) Autentifikatsiya jarayonini buzish

162. "Barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti".- Bular tarmoqning qaysi sathiga kiradi?

a) Fizik sath (physical)

b) Tarmoq sathi

c) Amaliy sath

d) Tadbiqiy sath

163. Bell-LaPadula (BLP) modeli -bu..

a) Bu hukumat va harbiy dasturlarda kirishni boshqarishni kuchaytirish uchun ishlatiladigan avtomatlashgan modeli

b) Axborlarni nazoratlovchi model

c) Foydalanuvchilarni ro‘yxatga olish , nazoratlash va tahlil qiluvchi model

d) Tarmoq boshqarish va tahlil qiluvchi model

164. Bell-LaPadula axborot xavfsizligida axborotni qaysi parametrini ta'minlash uchun xizmat qiladi?

a) Konfidentsiallikni

b) Yaxlitlikni

c) Maxfiylikni

d) O‘zgarmaslikni

165. Biba modeli obyektni qaysi xusuiyatiga e'tibor qaratilgan?

a) Yaxlitligi

b) Maxfiyligi

c) Xavfsizligi

d) Konfidentsialligi

166. BiBa modeli qaysi modelning keygaytirilgan varianti hisoblanadi?

a) Bell-Lapadula modeli

b) RBAC

c) MAC

d) ABAC

167. Biometrik parametrlarda xavfsizlik tomonidan kamchiligi nimadan iborat?

a) ID ni almashtirish murakkabligi

b) Foydalanish davrida maxfiylik kamayib boradi

c) Qalbakilashtirish oson

d) Parol va PIN kod ishlatilmasligi

168. Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang.

a) Shaxsiy simsiz tarmoq

b) Lokal simsiz tarmoq

c) Regional simsiz tarmoq

d) Global simsiz tarmoq

169. Botnet-nima?

a) internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi

b) zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi

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

d) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

170. …-bu so‘z ingliz tilidan olingan bo‘lib- yorib tashlash, chopish, buzish degan ma’nolarni anglatadi. Ular xaddan ziyod malakali va bilimli, axborot texnologiyalarini puxta biluvchi insondir.-Yuqoridagi fikr kim to‘g‘risida ta’rif berilgan?

a) Xaker

b) Dasturchi

c) Tarmoq josusi

d) Administrator

171. Bulutli texnologiyalarda PaaS nimani ifodalaydi?

a) Platforma sifatida

b) Servis sifatida

c) Ma'lumot sifatida

d) Prizentatsiya sifatida

172. GSM, GPRS, EDGE, HSPA+, LTE standartida ishlovchi simsiz tarmoq turini aniqlang.

a) Global simsiz tarmoq

b) Shaxsiy simsiz tarmoq

c) Lokal simsiz tarmoq

d) Regional simsiz tarmoq

173. Cloud Computing texnologiyasi nechta katta turga ajratiladi?

a) 3 turga

b) 2 turga

c) 4 turga

d) 5 turga

174. Dastur kodini tashkil qilish yondashuviga ko‘ra viruslar turlari?

a) Shifrlangan, shifrlanmagan, polimorf

b) Dasturiy, yuklanuvchi, makroviruslar, multiplatformali viruslar

c) Rezident, norezident

d) Virus parazit, virus cherv

175. Dasturiy shifrlash vositalari necha turga bo‘linadi?

a) 4

b) 3

c) 5

d) 6

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

a) Krakker

b) Hakker

c) Virus bot

d) Ishonchsiz dasturchi

177. DIR viruslari nimani zararlaydi?

a) FAT tarkibini zararlaydi

b) com, exe kabi turli fayllarni zararlaydi

c) yuklovchi dasturlarni zararlaydi

d) Operatsion tizimdagi sonfig.sys faylni zararlaydi

178. Diskni shifrlash nima uchun amalga oshiriladi?

a) Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi

b) Xabarni yashirish uchun amalga oshiriladi

c) Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi

d) Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi

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

a) Faglar

b) Detektorlar

c) Vaksinalar

d) Privivka

180. Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi.

a) Fizik sath (physical)

b) Kanal sath (data link)i

c) Tarmoq sathi

d) Transport sathi

181. Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?

a) raqamli imzoni shakllantirish va tekshirish muolajasi

b) raqamli imzoni hisoblash muolajasi

c) raqamli imzoni hisoblash va tekshirish muolajasi

d) raqamli imzoni shakllantirish muolajasi

182. Eng ko‘p axborot xavfsizligini buzilish xolati-bu:

a) Tarmoqda ruxsatsiz ichki foydalanish

b) Tizimni loyihalash xatolaridan foydalanish

c) Tashqi tarmoq resursiga ulanish

d) Simsiz tarmoqqa ulanish

183. Enterprise Information Security Policies, EISP-bu…

a) Tashkilot axborot xavfsizligi siyosati

b) Muammofa qaratilgan xavfsizlik siyosati

c) Tizimga qaratilgan xavfizlik siyosati

d) Maqbul foydalanish siyosati

184. Ethernet konsentratori(hub) qanday vazifani bajaradi?

a) kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo‘naltirib beradi

b) kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo‘naltirib beradi

c) kompyuterdan kelayotgan axborotni xalqa bo‘ylab joylashgan keyingi kompyuterga

d) tarmoqning ikki segmentini bir biriga ulaydi

185. Faol hujum turi deb nimaga aytiladi?

a) Maxfiy uzatish jarayonini uzib qo‘yish, modifikatsiyalash, qalbaki shifr ma’lumotlar tayyorlash harakatlaridan iborat jarayon

b) Maxfiy ma’lumotni aloqa tarmog‘ida uzatilayotganda eshitish, tahrir qilish, yozib olish

c) harakatlaridan iborat uzatilalayotgan ma’lumotni qabul qiluvchiga o‘zgartirishsiz yetkazish jarayoni

d) Ma’lumotga o‘zgartirish kiritmay uni kuzatish jarayoni

e) Sust hujumdan farq qilmaydigan jarayon

186. Faollashish prinspiga ko‘ra viruslar turlari?

a) Rezident, Norezident

b) Dasturiy, Makroviruslar, multiplatformali viruslar

c) Virus parazit, Virus cherv

d) Shifrlangan, shifrlanmagan, Polimorf

187. Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o‘zgarib turadigan parol nima deyiladi?

a) One-time password (OTP)

b) Only password (OP)

c) First Password (FP)

d) Primary Password (PP)

188. Faqat ma’lum hizmatlar /hujumlar/harakatlar bloklanadi. Bu qaysi xavfsizlik siyosatiga hos?

a) Ruxsat berishga asoslangan siyosat (Permissive Policy)

b) Ehtiyotkorlik siyosati (Prudent Policy)

c) Nomuntazam siyosat (Promiscuous Policy)

d) Paranoid siyosati (Paranoid Policy)

189. Fire Wall ning vazifasi...

a) Tarmoqlar orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta`minlaydi

b) kompyuterlar tizimi xavfsizligini ta`minlaydi

c) Ikkita kompyuter o‘rtasida aloqa o‘rnatish jarayonida Internet tarmog‘i orasida xavfsizlikni ta`minlaydi

d) uy tarmog‘i orasida aloqa o‘rnatish jarayonida tashkilot va Internet tarmog‘i orasida xavfsizlikni ta`minlaydi

190. Fizik to‘siqlarni o‘rnatish , Xavfsizlik qo‘riqchilarini ishga olish, Fizik qulflar qo‘yishni amalga oshirish qanday nazorat turiga kiradi?

a) Fizik nazorat

b) Texnik nazorat

c) Ma’muriy nazorat

d) Tashkiliy nazorat

191. Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi?

a) 2 taga

b) 4 taga

c) 3 taga

d) 5 taga

192. Fizik xavfsizlikni nazoratlashga nimalar kiradi?

a) Binoga to‘siqlar qo‘yish, eshikka qulflar o‘rnatish, xavfsizlik xodimlarini ishga olish.

b) Kompyuterlarga antivirus o‘rnatish, serverlarni ko‘paytirish, to‘siqlarni o‘rnatish

c) Hujjatlarni tashkillashtirish, xodimlarni o‘qitish,qulflarni o‘rnatish

d) Ruxsatni nazoratlash,shaxs xavfsizligini ta’minlash,muhitni nazoratlash

193. Foydalanish huquqini cheklovchi matritsa modeli bu...

a) Bella La-Padulla modeli

b) Dening modeli

c) Landver modeli

d) Huquqlarni cheklovchi model

194. Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari-bu…

a) Foydalanuvchanligi

b) Ma’lumotlar butunligi

c) Axborotning konfedensialligi

d) Ixchamligi

195. Foydalanishda boshqarishda ma’lumot , resurs, jarayon nima deb ataladi?

a) Obyekt

b) Subyekt

c) Tizim

d) Ruxsat

196. Foydalanishni boshqarish –bu...

a) Subyektni Obyektga ishlash qobilyatini aniqlashdir.

b) Subyektni Subyektga ishlash qobilyatini aniqlashdir.

c) Obyektni mizojga ishlash qobilyatini aniqlashdir

d) Autentifikatsiyalash jarayonidir

197. Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar qanday vazifani bajaradi?

a) Subyekt

b) Obyekt

c) Tizim

d) Ruxsat

198. Foydalanishni boshqarishda subyekt bu - ....

a) Inson, dastur, jarayon

b) Jarayon, dastur

c) Ma’lumot, resurs, jarayon

d) Resurs

199. Foydalanishni boshqarishning asosan nechta bor?

a) 4

b) 5

c) 6

d) 7

200. Foydalanishni boshqarishning ….. usuli tizimdagi shaxsiy obyektlarni himoyalash uchun qo‘llaniladi?

a) Discretionary access control( DAC)

b) Mandatory access control (MAC)

c) Role-based access control (RBAC)

d) Attribute based access control (ABAC)

201. Foydalanishni boshqarishning ….usulida foydalanishlar subyektlar va obyektlarni klassifikatsiyalashga asosan boshqariladi.

a) Mandatory access control (MAC)

b) Discretionary access control( DAC)

c) Role-based access control (RBAC)

d) Attribute based access control (ABAC)

202. Foydalanishni boshqarishning …. usulida ruxsatlar va xarakatni kim bajarayotganligi to‘g‘risidagi xolatlar “agar, u xolda” buyrug‘idan tashkil topgan qoidalarga asoslanadi.

a) Attribute based access control (ABAC)

b) Discretionary access control( DAC)

c) Mandatory access control (MAC)

d) Role-based access control (RBAC)

203. Foydalanishni boshqarishning …. usulida subyekt va obyektlarga tegishli huquqlarni ma’murlash oson kechadi.

a) Role-based access control (RBAC)

b) Discretionary access control( DAC)

c) Mandatory access control (MAC)

d) Attribute based access control (ABAC)

204. Foydalanishni boshqarishning …. usulida xavfsizlik markazlashgan tarzda xavfsizlik siyosati ma’muri tomonidan amalga oshiriladi.

a) Mandatory access control (MAC)

b) Discretionary access control( DAC)

c) Role-based access control (RBAC)

d) Attribute based access control (ABAC)

205. Foydalanishni boshqarishning Discretionary access control( DAC) usulidan asosan ….. qo‘llaniladi.

a) Operatsion tizimlarda

b) Ma’lumotlar bazasida

c) Web saytlarda

d) Kompyuter tarmoqlarda

206. Tarmoqda foydalanuvchilarga tegishli ma’lumotlarini qo‘lga kiritub, uni hujum qiluvchiga yuboraradigan dasturiy kod qanday ataladi?

a) Spyware

b) Rootkits

c) Backdoors

d) Ransomware

207. Kompyuter tarmoqdagi foydalanuvchilar harakatini, uning axborot resurslardan foydalanishga urinishini qayd etish qansi atama bilan nomlanadi?

a) Ma’murlash

b) Identifikatsiyalash

c) Autentifikatsiyalash

d) Aniqlash

208. Global tamoq dastlab paytda qaysi nom bilan atalgan?

a) ARPANET

b) NETWORK

c) INTRANET

d) INTERNET

209. ….-mavjud tahdidni amalga oshirilgan ko‘rinishi bo‘lib, bunda kutilgan tahdid amalga oshiriladi.

a) Hujum

b) Tahdid

c) Zaiflik

d) Buzish

210. Identifikatsiya va autentifikatsiyadan o‘tgan foydalanuvchilarga tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni – bu…

a) Avtorizatsiya

b) Identifikatsiya

c) Autentifikatsiya

d) Ma’murlash

211. IEEE 802.11, Wi-Fi standartini qo‘llovchi tarmoq turini aniqlang.

a) Lokal simsiz tarmoq

b) Shaxsiy simsiz tarmoq

c) Regional simsiz tarmoq

d) Global simsiz tarmoq

212. IEEE 802.16, WiMAX standartini qo‘llovchi tarmoq turini aniqlang.

a) Shahar simsiz tarmoq

b) Shaxsiy simsiz tarmoq

c) Lokal simsiz tarmoq

d) Global simsiz tarmoq

213. Elektron imzoni haqiqiyligini tekshirish … amalga oshiriladi.

a) Imzo muallifining ochiq kaliti yordamida

b) Ma’lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida

c) Ma’lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida

d) Imzo muallifining maxfiy kaliti yordamida

214. DoS hujumlari oqibati quyidagilardan qaysi biri sodir bo‘ladi?

a) Foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan mahrum qilinadilar

b) Foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzg‘unchilarga etkaziladi

c) Axborot tizimidagi ma’lumotlar bazalari o‘g‘irlanib ko‘lga kiritilgach, ular yo‘q qilinadilar

d) Foydalanuvchilar axborotlariga ruxsatsiz o‘zgartirishlar kiritilib, ularning yaxlitligi buziladi

215. Kriptografiga “Kalit” atamasiga qanday ta’rif beriladi?

a) axborotni shifrlash va deshifrlash uchun kerakli axborot

b) Bir qancha kalitlar yig‘indisi

c) Axborotli kalitlar to‘plami

d) Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

216. Kalitlar boshqaruvi qanday elementga ega bo‘ladi?

a) hosil qilish, yig‘ish, taqsimlash

b) ishonchliligi, maxfiyligi, aniqligi

c) xavfsizlik, tez ishlashi, to‘g‘ri taqsimlanishi

d) abonentlar soni, xavfsizligi, maxfiyligi

217. Kiberxavfsizkda “tahdid” atamasi qanday ta’riflanadi?

a) Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa

b) Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa

c) Bu riskni o‘zgartiradigan harakatlar

d) Bu noaniqlikning maqsadlarga ta’siri

218. Kiberxavfsizlik nechta bilim soxasini o‘z ichiga oladi?

a) 8 ta

b) 6 ta

c) 5 ta

d) 7 ta

219. Kiberxavfsizlikni ta’minlash masalalari bo‘yicha xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang.

a) SANS (System Administration Networking and Security)

b) Department of defence (DOD)

c) Discretionary access control

d) Attribute based access control

220. Kimlar o‘zining harakatlari bilan sanoat josusi yetkazadigan muammoga teng (undan ham ko‘p bo‘lishi mumkin) muammoni yuzaga keltiradi?

a) Ishonchsiz xodimlar

b) Xaker-proffesional

c) Sarguzasht qidiruvchilar

d) G‘oyaviy xakerlar

221. 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?

a) Kiberetika

b) Kiberhuquq

c) Kiberqoida

d) Kiberxavfsizlik

222. Tarmoq qurilmalari IPv4 manzilni to‘g‘ri kiritilishini ko‘rsating.

a) 172.25.100.100

b) 12:AC:14:1C:3B:13

c) 255.255.255.0

d) 1001000110111

223. Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi…

a) Kompyuter tarmoqlari

b) Kompyuter markazi

c) Ma’lumotlar bazasi

d) Tarmoq xavfsizligi

224. ….kompyuter tizimiga tahdid qilish imkoniyatiga ega va troyanlar, viruslar, “qurt”lar ko‘rinishida bo‘lishi mumkin.

a) Zararli dastur

b) .exe fayl

c) Boshqariluvchi dastur

d) Kengaytmaga ega bo‘lgan fayl

225. ….bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida o‘zini ko‘rsatsada, yashiringan zararli koddan iborat.

a) troyan otlari

b) adware

c) spyware

d) rootkits

226. ….zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi.

a) mantiqiy bombalar

b) adware

c) spyware

d) rootkits

227. ….keng qamrovli nishondagi tizim va tarmoq resurlarida xizmatdan foydalanishni buzishga qaratilgan hujum bo‘lib, Internetdagi ko‘plab zombi kompyuterlar orqali bilvosita amalga oshiriladi.

a) Taqsimlangan DOS hujumlar

b) O‘rtada turgan odam hujumi

c) Parolga qaratilgan hujumlar

d) Passiv razvedka hujumlari

228. Qaysi hujumlar asosan portlarni va operaesion tizimni skanerlashni maqsad qiladi?

a) Aktiv razvedka hujumlari

b) O‘rtada turgan odam hujumi

c) Parolga qaratilgan hujumlar

d) Passiv razvedka hujumlari

229. …. hujumlari trafik orqali axborotni to‘plashga harakat qiladi. Buning uchun hujumchi sniffer deb nomlanuvchi dasturiy vositadan foydalanadi.

a) Passiv razvedka hujumlari

b) Aktiv razvedka hujumlari

c) O‘rtada turgan odam hujumi

d) Parolga qaratilgan hujumlar

230. …. nishondagi kompyuter tizimi uchun nazoratni qo‘lga kiritish yoki ruxsatsiz foydalanish maqsadida amalga oshiriladi.

a) Passiv razvedka hujumlari

b) Aktiv razvedka hujumlari

c) O‘rtada turgan odam hujumi

**d) Parolga qaratilgan hujumlar**

231. … hujumda hujum qiluvchi o‘rnatilgan aloqaga suqilib kiradi va aloqani uzadi.

a) Passiv razvedka hujumlari

b) Aktiv razvedka hujumlari

**c) O‘rtada turgan odam hujumi**

d) Parolga qaratilgan hujumlar

232. Konfidentsial axborotdan foydalanish tushunchasi…

a) Muayyan shaxsga tarkibida konfidensial xarakterli ma’lumot bo‘lgan axborot bilan tanishishga vakolatli mansabdor shaxsning ruxsati.

b) Korxona o‘z faoliyatini buzilishsiz va to‘xtalishsiz yurgiza oladigan vaqt bo‘yicha barqaror bashoratlanuvchi atrof-muhit holati.

c) Ma’lumotlarning ma’lumotlar bazasiga tegishli darajasini aniqlash va belgilash.

d) Olingan ma’lumotlar jo‘natuvchisining so‘ralganiga mosligini tasdiqlash

233. Kriptoanaliz qanday jarayonlarni o‘rganadi?

a) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

b) axborotni qayta akslantirishning texnik usullarini izlaydi va tadqiq qiladi

c) axborotni akslantirib himoyalash muammosi bilan shug‘ullanadi

d) kalitni qo‘llab matnni ochish imkoniyatlarini o‘rganadi

234. Kriptografiya qanday jarayonlarni o‘rganadi?

a) axborotni akslantirish va qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

b) axborotni qayta akslantirib himoyalash muammosi bilan shug‘ullanadi

c) kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi

d) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

235. Kriptologiya nechta yo‘nalishga bo‘linadi?

a) 2 ta

b) 3 ta

c) 4 ta

d) 5 ta

236. Kompyuter tarmoqlarda qo‘llanuvchi topologiya turi qaysi?

a) Yulduz, shina, xalqa

b) Markaziy, tengma-teng, aralash

c) To‘liq bog‘langan, shina, aylana

d) Shina, optik, koaksial

237. Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish jarayoni qanday ataladi?

a) Autentifikatsiya

b) Identifikatsiya

c) Ma’murlash (accaunting)

d) Avtorizatsiya

238. Qog‘oz ma’lumotlarni yo‘q qilish odatda necha xil usulidan foydalaniladi?

a) 4 xil

b) 8 xil

c) 7 xil

d) 5 xil

239. Ma’lumotlarni zaxira nusxalash bu – …

a) Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni

b) Axborotni turli dasturlar yordamida tiklash imkoniyati

c) Ma’lumotlarni ishonchli o‘chirish imkoniyati

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

240. Turli offis ilovalari – MS Word hujjati, MS Excel elektron jadvali kabi fayllarni qaysi virus turi zararlaydi?

a) Makroviruslar

b) Troyanlar

c) Botnetlar

d) Mutantvirus

241. Ma'lumotlarni zahira nusxasini saqlovchi va qayta tikovchi dasturni belgilang.

a) Redo Backup and Recovery

b) BestCrypt

c) Cryptool 1.4

d) Eset32

242. Nomuntazam siyosat (Promiscuous Policy) nima?

a) Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi

b) Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi

c) Hamma narsa taqiqlanadi

d) Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

243. OSI modelining birinchi sathi nomini belgilang.

a) Fizik sath (physical)

b) Ilova sath (application)

c) Seans sath (session)

d) Kanal sath (data link)

244. OSI modelining ikkinchi sathi nomini belgilang .

a) Kanal sath (data link)

b) Fizik sath (physical)

c) Ilova sath (application)

d) Seans sath (session)

245. OSI modelining uchinchi sathi nomini belgilang .

a) Tarmoq(network)

b) Fizik sath (physical)

c) Ilova sath (application)

d) Seans sath (session)

246. OSI modelining to‘rtinchi sathi nomini belgilang .

a) Transport (transport)

b) Fizik sath (physical)

c) Ilova sath (application)

d) Taqdimot (presentation)

247. OSI modelining beshinchi sathi nomini belgilang.

a) Seans sath (session)

b) Fizik sath (physical)

c) Ilova sath (application)

d) Seans sath (session)

248. OSI modelining oltinchi sathi nomini belgilang.

a) Taqdimot (presentation)

b) Fizik sath (physical)

c) Ilova sath (application)

d) Tarmoq(network)

249. OSI modelining yettinchi sathi nomini belgilang

a) Ilova sath (application)

b) Seans sath (session)

c) Fizik sath (physical)

d) Tarmoq(network)

250. OSI modelida nechta sathdan iborat?

a) 7 ta

b) 4 ta

c) 5 ta

d) 3 ta

251. OSI modelining Ilova sath (application) sathida qanday protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket

b) ASCII, EBCDIC, JPEG, MIDI

c) TCP, UDP, SCTP

d) IPv4, IPv6, IPsec, AppleTalk, ICMP

252. OSI modelining Taqdimot (presentation) sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket

**b) ASCII, EBCDIC, JPEG, MIDI**

c) TCP, UDP, SCTP

d) IPv4, IPv6, IPsec, AppleTalk, ICMP

253. OSI modelining Transport sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket

b) ASCII, EBCDIC, JPEG, MIDI

**c) TCP, UDP, SCTP**

d) IPv4, IPv6, IPsec, AppleTalk, ICMP

254. OSI modelining Tarmoq (network) sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket

b) ASCII, EBCDIC, JPEG, MIDI

c) TCP, UDP, SCTP

**d) IPv4, IPv6, IPsec, AppleTalk, ICMP**

255. OSI modelining Kanal (data link) sathida qaysi protokollar ishlaydi?

a) HTTP, FTP, POP3, SMTP, WebSocket

b) ASCII, EBCDIC, JPEG, MIDI

c) TCP, UDP, SCTP

**d) PPP, IEEE 802.22, Ethernet, DSL, ARP**

256. OSI modelining Fizik (physical) sathida qanday tarmoq qurilmalari qo‘llaniladi?

a) Marshrutizator

b) Ko‘prik

c) Tarmoq adapter

**d) Kontsentrator**

257. OSI modelining Kanal (data link) sathida qanday tarmoq qurilmalar qo‘llaniladi?

a) Marshrutizator

b) Ko‘prik

c) Tarmoq ekrani

**d) Kommutator**

258. OSI modelining Tarmoq (network) sathida qanday tarmoq qurilmalar qo‘llaniladi?

**a) Marshrutizator**

b) Ko‘prik

c) Tarmoq ekrani

d) Kommutator

259. OSI modelining Fizik (physical) sathida axborot tipi qanday nomlanadi?

**a) bit**

b) kadr

c) paket

d) segmet

260. OSI modelining Kanal (data link) sathida axborot tipi qanday nomlanadi?

a) ma’lumot

**b) bit/kadr**

c) paket

d) segmet/datagramma

261. OSI modelining Tarmoq (network) sathida axborot tipi qanday nomlanadi?

a) ma’lumot

b) bit/kadr

**c) paket**

d) segmet/datagramma

262. OSI modelining Transport sathida axborot tipi qanday nomlanadi?

a) ma’lumot

b) bit/kadr

c) paket

**d) segmet/datagramma**

263. Paranoid siyosati (Paranoid Policy) – bu ….

**a) Hamma narsa ta’qiqlanadi**

b) Tizim resurslaridan foydalanishda hech qanday cheklovlar qo‘ymaydi

c) Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi

d) Barcha hizmatlar blokirovka qilingandan so‘ng bog‘lanadi

264. Polimorf viruslar tushunchasi to‘g‘ri ko‘rsating.

a) Viruslar turli ko‘rinishdagi shifrlangan viruslar bo‘lib, o‘zining ikkilik shaklini nusxadan-nusxaga o‘zgartirib boradi

b) Odatda foyl tarkibida yashirinib tarqaydi

c) o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dasturkodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi

d) Viruslar yuklangan qattiq diskdagi, disketa yoki fleshkasektorlarida joylashgan kichik programmalarni zararlaydi yoki uni almashtiradi.

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

a) Shaxsiy tarmoq

b) Lokal

c) Mintaqaviy

d) Campus

266. Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi?

a) DNS tizimlari

b) TCP/IP

c) Ethernet

d) Token ring

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

a) Razvedka hujumlari

b) Kirish hujumlari

c) DOS hujumlari

d) Zararli hujumlar

268. Qanday hujumda hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi?

a) Kirish hujumlari

b) Razvedka hujumlari

c) DOS hujumlar

d) Zararli hujumlar

269. Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi?

a) Tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi

b) Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi

c) Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.

d) Potensial zaiflikni aniqlash imkoniyati yo‘qligi

270. Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi?

a) Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi

b) Tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi

c) Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.

d) Potensial zaiflikni aniqlash imkoniyati yo‘qligi

271. Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi?

a) Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi.

b) Tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi

c) Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi

d) Potensial zaiflikni aniqlash imkoniyati yo‘qligi

272. Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.

a) Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.

b) Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.

c) Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi

d) Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi

273. Quyidagilardan MAN (metropolitan area network) tarmoqqa berilgan ta’rifni belgilang.

a) Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi

b) Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.

c) Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.

d) Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi

274. Kompyuter tarmoqlaridan “Umumiy shina” topologiyasi xususiyati qanday?

a) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi

b) Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi

c) Yuboriluvchi va qabul qilinuvchi ma’lumot token yordamida manziliga yetkaziladi

d) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi

275. Kompyuter tarmoqlaridan “Yulduzsimon” topologiyasiga ta'rif bering.

a) Har bir kompyuterni markaziy konsentrator bilan ulash orqali tashkil etiladi

b) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi

c) Yuboriluvchi va qabul qilinuvchi ma’lumot token yordamida manziliga yetkaziladi

d) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi

276. Kompyuter tarmoqlaridan “Xalqasimon” topologiyasiga ta'rif bering.

a) Har bir kompyuter boshqa ikkita kompyuter bilan ulangan va signal aylana bo‘yicha o‘tadi

b) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi

c) Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi

d) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi

277. Quyidagilardan qaysi birida tarmoqning “Uyali mesh” topologiyasiga ta'rif berilgan?

a) Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi

b) Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi

c) Yuboriluvchi va qabul qilinuvchi ma’lumot Token yordamida manziliga yetkaziladi

d) Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi

278. Aksariyat tashkilotlar muhim ma’lumotlarini qaysi texnologiyasi asosida zaxira nusxalashni amalga oshiradilar?

a) Random Array of Independent Disks(RAID)

b) Virtual private network(VPN)

c) Point to Point

d) HyperText Transfer Protocol(HTTP)

279. Ransomware zararli dasturi axborotlarga qanday zarar keltiradi?

a) mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi.

b) marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.

c) foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.

d) bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi.

280. Ma ’murlash usuli bo‘yicha tarmoqlar qanday turlarga bo‘linadi?

a) “Bir rangli” va “mijoz server” turlarga

b) Server va kliyent turlarga

c) Asosiy va qo‘shimcha turlar

d) Korporativ va xalqaro turlarga

281. Rezident bo‘lmagan viruslar qachon xotirani zararlaydi?

a) Faqat faollashgan vaqtida

b) Faqat o‘chirilganda

c) Kompyuter yoqilganda

d) Tarmoq orqali ma’lumot almashishda

282. Risk, tahdid, zaiflik va ta’sir tushunchalari o‘rtasida o‘zaro bog‘lanish qanday ifodalanadi?

a) RISK = Tahdid x Zaiflik x Ta’sir

b) RISK = Tahdid +Zaiflik + Ta’sir

c) RISK = Tahdid x (Zaiflik +Ta’sir)

d) RISK = Tahdid -Zaiflik +Ta’sir

283. Risk darajasi tarmoqga (yoki tizimga) natijaviy ta’sirning bahosi bo‘lib, quyidagi tenglik bilan ifodalanadi:

a) Risk darajasi = natija \* ehtimollik

b) Risk darajasi = natija +ehtimollik.

c) Risk darajasi = natija /ehtimollik.

d) Risk darajasi = natija - ehtimollik.

284. Samarali risklarni boshqarishning rejasi risklarni aniqlashni va baholashni kafolatli amalga oshirishda …. va qayta ko‘rib chiqishni talab etadi.

a) Risk monitoringi

b) Riskni tahlillash

c) Muvaffaqiyatli risklar

d) Tanazzulga uchragan risklar

285. Risk darajalari nechta turga bo‘linadi?

a) 4 ta

b) 3 ta

c) 2 ta

**d) 5 ta**

286. Risklarni boshqarish –bu…

a) Risklarni aniqlash, baholash, javob berish va bo‘lishi mumkin bo‘lgan ta’sirga tashkilot tomonidan javob berilishini amalga oshirish jarayoni

b) Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta’siri va ehtimolini o‘lchashni ta’minlaydi.

c) Aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni.

d) Risk monitoringi yangi risklarni paydo bo‘lish imkoniyatini aniqlash

287. Risklarni boshqarish jarayoni quyidagi asosiy nechta bosqichga ajratiladi?

a) 4 ta

b) 2 ta

c) 5 ta

d) 3 ta

288. …. tashkilotning risklarni boshqarish usuliga amalga oshirish tadbirlarini belgilaydi va tashkilotda axborot xavfsizligi va risklarni boshqarish bo‘yicha faoliyatni birlashtimvchi tarkibiy jarayonni ta’minlaydi.

a) Risklarni boshqarish freymworki

b) Risk monitoringi

c) Riskni tahlillash

d) Muvaffaqiyatli risklar

289. Rootkitlar qanday zararli amallar bajaradi?

a) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi

b) bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi

c) o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi

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

290. 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?

a) Fizik nazorat

b) Huquqiy nazorat

c) Ma’muriy nazorat

d) Tashkiliy nazorat

291. Shifrlash nima?

a) ochiq matnni shifrmatnga o‘zgartirish jarayoni

b) shifrmatnni ochiq matnga o‘zgartiruvchi teskari jarayoni

c) kalitni bilmasdan turib shifrmatn bo‘yicha ochiq matnni tiklash jarayoni

d) alfavit elementlaridan tartiblangan nabor

292. Kriptotizim bu-…

a) ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o‘zgartirishlar oilasi

b) shifrmatnni ochiq matnga o‘zgartiruvchi teskari jarayoni

c) kalitni bilmasdan turib shifrmatn bo‘yicha ochiq matnni tiklash jarayoni

d) alfavit elementlaridan tartiblangan nabor

293. Simmetrik kriptotizimlarda ... .

a) shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi

b) bir-biriga matematik usullar bilan bog‘langan ochiq va yopiq kalitlardan foydalaniladi

c) axborot ochiq kalit yordamida shifrlanadi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi

d) kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi

294. Simsiz tarmoqlarni kategoriyalarini to‘g‘ri ko‘rsating?

a) Simsiz shaxsiy tarmoq, simsiz lokal tarmoq, simsiz shahar tarmoq va simsiz global tarmoq

b) Simsiz internet tarmoq va Simsiz telefon tarmoq, Simsiz shaxsiy tarmoq va Simsiz global tarmoq

c) Simsiz internet tarmoq va uy simsiz tarmog‘i

d) Simsiz chegaralanmagan tarmoq , simsiz kirish nuqtalari

295. Spyware-qanday zararli dastur?

a) tarmoqda foydalanuvchilarga tegishli ma’lumotlarini qo‘lga kiritub, uni hujum qiluvchiga yuboraradigan dasturiy kod

b) ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

c) internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi

d) zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi

296. Subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim qilish jarayoni nima?

a) Identifikatsiya

b) Autentifikatsiya

c) Avtorizatsiya

d) Ma’murlash

297. Kompyuter virusining birinchi ta’rifni kim bergan?

a) 1984 yili Fred Koen

b) 1951 yil Jon fon Neumann

c) 1981 yil Elik Cloner

d) 1990 yil Bill Geyts

298. Kompyuter viruslari hayot davrining ikkita asosiy bosqichini toping.

a) Saqlanish va bajarilish

b) Yaralish va yashash

c) Tarqalish va zararlash

d) Zararlash va yo‘q bo‘lish

299. Kompyuter viruslarining bajarilish davri, odatda, nechta bosqichni o‘z ichiga oladi?

a) 5 ta

b) 2 ta

c) 3 ta

d) 4 ta

300. O‘z-o‘zidan tarqalish mexanizmi amalga oshiriluvchi, tizimga zarar keltirmaydi, faqat diskdagi bo‘sh xotirani sarflaydigan viruslar qanday viruslar deb ataladi?

a) Beziyon viruslar

b) Xavfsiz viruslar

c) Xavfli viruslar

d) Juda xavfli viruslar

301. Tizimda mavjudligi turli taassurot (ovoz, video) bilan bog‘liq, bo‘sh xotirani kamaytirsada, dastur va ma’lumotlarga ziyon yetkazmaydigan viruslar qanday viruslar deb ataladi?

a) Xavfsiz viruslar

b) Beziyon viruslar

c) Xavfli viruslar

d) Juda xavfli viruslar

302. Kompyuter ishlashida jiddiy nuqsonlarga sabab bo‘luvchi, natijada dastur va ma’lumotlar buzilishiga olib kelivchi viruslar qanday viruslar deb ataladi?

a) Xavfli viruslar

b) Xavfsiz viruslar

c) Beziyon viruslar

d) Juda xavfli viruslar

303. PPP-kadrlarni tarmoq sathi paketlariga inkapsulyatsiyalovchi kanal sathining tunnel protokolini belgilang.

a) L2TP (Layer 2 Tunneling Protocol)

b) IPSec (IP Security)

c) PPTP (Point-to-Point Tunneling Protocol)

d) SSH (Secure Shell)

304. “nuqta-nuqta” xilidagi kanal sathining tunnel protokolini belgilang.

a) IPSec (IP Security)

b) PPTP (Point-to-Point Tunneling Protocol)

c) SSH (Secure Shell)

d) L2TP (Layer 2 Tunneling Protocol)

305. Tarmoqlararo ekran (firewall, brandmaver) –bu…

a) Trafikni filtrlash mexanizmiga asoslangan tarmoqdan foydalanishni cheklashning bazaviy vositasi

b) Qurilma perimetrli himoyalash masalasining kompleks yechimi hisoblanadi

c) Ma’lumotlarni inkapsulyatsiyalash mexanizmlari, hamda qo‘shimcha autentifikatsiya, shifrlash, yaxlitlikni nazoratlash

306. Kiruvchi ma’lumotning uzunligi o‘zgaruvchan, chiqishda esa o‘zgarmas uzunlikdagi qiymatni qaytaradigan jarayon qanday ataladi?

a) Xesh funksiya

b) О‘rniga qoyish akslantirish

c) O‘rin almashtirish akslantirishi

d) Elektron raqamli imzo

307. Ochiq matn simvollari bir alfavitdan olinib, unga mos shifrmatn simvollari boshqa bir alfavitdan olinadigan jarayon nomini belgilang.

a) О‘rniga qoyish akslantirish

b) Xesh funksiya

c) O‘rin almashtirish akslantirishi

d) Elektron raqamli imzo

308. Ochiq matnda ishtirok etgan simvollar shifrmatnda ham ishtirok etib, faqat ularning o‘rnii almashadigan jarayon nomini belgilang.

a) O‘rin almashtirish akslantirishi

b) О‘rniga qoyish akslantirish

c) Xesh funksiya

d) Elektron raqamli imzo

309. …. ashkilotning va u bilan bog‘liq boshqa komponentlar va interfeyslarning istalgan axborot xavfsizligi tizimi xolatini tavsiflaydi.

a) Kiberxavfsizlik arxitekturasi

b) Kiberxavfsizlik siyosati

c) Simmetrik shiflash

d) Elektron raqamli imzo

310. Fishing hujumi usullari to‘g‘ri ko‘rsatilgan qatorni belgilang: 1.Soxta havola; 2.soxta lotereya; 3.TV reklama; 4. Tekin dasturlar; 5.DOS hujum 6.Razvedka

a) 1,2,4

b) 2,3,5

c) 3,5,6

d) 4,5,6

Xato

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

Paranoid siyosat

Zаxirаlаshning qаndаy turlаri mаvjud?

Ichki, tаshqi

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

Dаstlаbki virus nechаnchi yildа yarаtilgаn?

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](http://moodle.fbtuit.uz/mod/url/view.php?id=19891) 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

1. Rezident virus…

tezkor xotirada saqlanadi

1. 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

1. O‘chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.

Recuva, R.saver

1. Zaiflik – bu…

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

1. Axborot xavfsizligi timsollarini ko‘rsating.

Alisa, Bob, Eva

1. Kiberetika tushunchasi:

Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

1. "Axborot olish va kafolatlari va erkinligi to‘g‘risda"gi Qonuni qachon kuchga kirgan?

1997 yil 24 aprel

1. DIR viruslari nimani zararlaydi?

FAT tarkibini zararlaydi

1. 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

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

"Issiq zaxiralash"

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

Tamoqlararo ekranlarning o‘rnatilishi

1. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

Axborot xavfsizligi buzulgan taqdirda ko‘rilishi mumkin bo‘lgan zarar miqdori bilan

1. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…

Kiberjinoyat deb ataladi

1. Antiviruslarni, qo‘llanish usuliga ko‘ra... turlari mavjud?

detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar

1. Qaysi siyosatga ko‘ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?

Ruxsat berishga asoslangan siyosat

1. DIR viruslari nimani zararlaydi?

FAT tarkibini zararlaydi

1. 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.

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

HandyBakcup

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

"Sovuq saxiralash"

1. “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

1. 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

1. 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.

|  |  |  |
| --- | --- | --- |
|  | Xavfsizlikning asosiy yo’nalishlarini sanab o’ting. | Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik |
|  | Axborot xavfsizligining asosiy maqsadlaridan biri- bu… | Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish |
|  | Konfidentsiallikga to’g’ri ta`rif keltiring. | axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; |
|  | Yaxlitlikni buzilishi bu - … | Soxtalashtirish va o’zgartirish |
|  | ... axborotni himoyalash tizimi deyiladi. | Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi |
|  | Kompyuter virusi nima? | maxsus yozilgan va zararli dastur |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya mahnosi... | sirli yozuv |
|  | Kriptologiya yo’nalishlari nechta? | 2 |
|  | Kriptografiyaning asosiy maqsadi... | maxfiylik, yaxlitlilikni ta`minlash |
|  | SMTP - Simple Mail Transfer protokol nima? | elektron pochta protokoli |
|  | SKIP protokoli... | Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi |
|  | Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar… | uzilish, tutib qolish, o’zgartirish, soxtalashtirish |
|  | ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. | konfidentsiallik |
|  | Foydalanish huquqini cheklovchi matritsa modeli bu... | Bella La-Padulla modeli |
|  | Kommunikatsion qism tizimlarida xavfsizlikni ta`minlanishida necha xil shifrlash ishlatiladi? | 2 |
|  | Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? | TCP/IP, X.25 protokollar |
|  | Himoya tizimi kompleksligiga nimalar orqali erishiladi? | Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali |
|  | Kalit – bu … | Matnni shifrlash va shifrini ochish uchun kerakli axborot |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | simmetrik kriptotizimlar |
|  | Autentifikatsiya nima? | Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi |
|  | Identifikatsiya bu- … | Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni |
|  | O’rin almashtirish shifri bu - … | Murakkab bo’lmagan kriptografik akslantirish |
|  | Simmetrik kalitli shifrlash tizimi necha turga bo’linadi. | 2 turga |
|  | Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular … | hosil qilish, yig’ish, taqsimlash |
|  | Kriptologiya - | axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi |
|  | Kriptografiyada alifbo – | axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam |
|  | Simmetrik kriptotizimlarda ... jumlani davom ettiring | shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi |
|  | Kriptobardoshlilik deb … | kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Elektron raqamli imzo deb – | xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha |
|  | Kriptografiya – | axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi |
|  | Kriptografiyada matn – | alifbo elementlarining tartiblangan to’plami |
|  | Kriptoanaliz – | kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Shifrlash – | akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi |
|  | Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi? | Tez, aniq va maxfiyligiga |
|  | Faol hujum turi deb… | Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon |
|  | Blokli shifrlash- | shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish |
|  | Simmetrik kriptotizmning uzluksiz tizimida … | ochiq matnning har bir harfi va simvoli alohida shifrlanadi |
|  | Kripto tizimga qo’yiladigan umumiy talablardan biri | shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak |
|  | Quyidagi tengliklardan qaysilari shifrlash va deshifrlashni ifodalaydi? | Ek1(T)=T, Dk2(T1)=T |
|  | Berilgan ta`riflardan qaysi biri assimmetrik tizimlarga xos? | Assimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi |
|  | Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang | Vijiner matritsasi, Sezar usuli |
|  | Akslantirish tushunchasi deb nimaga aytiladi? | 1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga |
|  | Simmetrik guruh deb nimaga aytiladi? | O’rin almashtirish va joylashtirish |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | simmetrik kriptositemalar |
|  | Xavfli viruslar bu - … | kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Elektron raqamli imzo tizimi qanday muolajani amalga oshiradi? | raqamli imzoni shakllantirish va tekshirish muolajasi |
|  | Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? | Simmetrik va assimetrik |
|  | Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin? | Korporativ va umumfoydalanuvchi |
|  | Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo’linadi? | Sust va faol |
|  | Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? | SMTP, POP yoki IMAR |
|  | Axborot resursi – bu? | axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi |
|  | Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu? | login |
|  | Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu? | parol |
|  | Identifikatsiya jarayoni qanday jarayon? | axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni |
|  | Autentifikatsiya jarayoni qanday jarayon? | ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash |
|  | Avtorizatsiya jarayoni qanday jarayon? | foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni |
|  | Ro’yxatdan o’tish bu? | foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni |
|  | Axborot qanday sifatlarga ega bo’lishi kerak? | ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | bit |
|  | Elektronhujjatning rekvizitlari nechta qismdan iborat? | 4 |
|  | Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? | fleshka, CD va DVD disklar |
|  | Imzo bu nima ? | hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati. |
|  | Muhr bu nima? | hujjatning haqi-qiyligini va biror bir yuridik shaxsga tegishli ekanligi-ni tasdiqlovchi isbotdir. |
|  | DSA – nima | Raqamli imzo algoritmi |
|  | El Gamal algoritmi qanday algoritm | Shifrlash algoritmi va raqamli imzo algoritmi |
|  | Sezarning shifrlash sistemasining kamchiligi | Harflarning so’zlarda kelish chastotasini yashirmaydi |
|  | Axborot xavfsizligi va xavfsizlik san’ati haqidagi fan …. deyiladi? | Kriptografiya |
|  | Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu - | steganografiya |
|  | Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? | Deshifrlash |
|  | …… – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. | Kiberxavfsizlik |
|  | Risk | Potensial foyda yoki zarar |
|  | Kiberxavfsizlik nechta bilim soxasini o‘z ichiga oladi. | 8 |
|  | “Ma’lumotlar xavfsizligi” bilim sohasi...... | ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi. |
|  | “Dasturiy ta’minotlar xavfsizligi” bilim sohasi..... | foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi. |
|  | “Tashkil etuvchilar xavfsizligi” ..... | katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi. |
|  | “Aloqa xavfsizligi” bilim sohasi...... | tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi. |
|  | “Tizim xavfsizligi” bilim sohasi…… | tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi. |
|  | “Inson xavfsizligi” bilim sohasi…. | kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi. |
|  | “Tashkilot xavfsizligi” bilim sohasi …. | tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini |
|  | “Jamoat xavfsizligi” bilim sohasi ….. | u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi. |
|  | Tahdid nima? tizim yoki | Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
|  | Kodlash nima? | Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir |
|  | Shifrlash nima? | Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi |
|  | Bir martalik bloknotda Qanday kalitlardan foydalaniladi? | Ochiq kalitdan |
|  | Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing. | 23 |
|  | Agar RSA algotirmida n ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi. | M = Cd mod n; |
|  | O’nlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq tizi miga o’tkazing. 65 | 100001 |
|  | Quyidagi modulli ifodani qiymatini toping. (125\*45)mod10. | 5 |
|  | Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256. | 244 |
|  | Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi. | C = Me mod n; -tog’ri javob |
|  | Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi | Kriptologiya. |
|  | Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi | {*d, n*} – yopiq, {*e, n*} – ochiq; |
|  | Zamonaviy kriptografiya qanday bo’limlardan iborat? | Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish |
|  | 1.      Kriptografik usullardan foydalanishning asosiy yo’nalishlari nimalardan iborat? | Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarni haqiqiyligini aniqlash, tashuvchilarda axborotlarni shifrlangan ko’rinishda saqlash (masalan, hujjatlarni, ma’lumotlar bazasini) |
|  | Shifr nima? | Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm |
|  | Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? | Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi |
|  | Oqimli shifrlashning mohiyati nimada? | Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur, Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi |
|  | Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating. | uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim, |
|  | Kriptotizim quyidagi komponentlardan iborat: | ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, Ek : M ® C (shifrlash uchun) va Dk: C®M (deshifrlash uchun) funktsiyalar |
|  | Serpent, Square, Twofish, RC6 , AES algoritmlari qaysi turiga mansub? | simmetrik blokli algoritmlar |
|  | DES algoritmiga muqobil bo’lgan algoritmni ko’rsating. | Uch karrali DES, IDEA, Rijndael |
|  | DES algoritmining asosiy muammosi nimada? | kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas |
|  | Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? | shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun |
|  | 12+22 mod 32 ? | 2 |
|  | 2+5 mod32 ? | 7 |
|  | Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi. | ochiq kalitlar |
|  | 12+11 mod 16 ? | 7 |
|  | RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo’llab quvvatlaydi. | 128 bitli, 192 bitli, 256 bitli |
|  | Xesh-funktsiyani natijasi … | uzunlikdagi xabar |
|  | RSA algoritmi qanday jarayonlardan tashkil topgan | Kalitni generatsiyalash; Shifrlash; Deshifrlash. |
|  | RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida necha bit bo‘lishi talab etiladi. | 2048 |
|  | Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi | Xesh funksiyalar |
|  | To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub | Xalqa |
|  | Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo’llamasligi mumkin | to’liq bog’lanishli |
|  | Kompyuterning tashqi interfeysi deganda nima tushuniladi | kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari |
|  | Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi | Yulduz |
|  | Ethernet kontsentratori qanday vazifani bajaradi | kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi |
|  | OSI modelida nechta sath mavjud | 7 |
|  | OSI modelining to’rtinchi sathi qanday nomlanadi | Transport sathi |
|  | OSI modelining beshinchi sathi qanday nomlanadi | Seanslar sathi |
|  | OSI modelining birinchi sathi qanday nomlanadi | Fizik sath |
|  | OSI modelining ikkinchi sathi qanday nomlanadi | Kanal sathi |
|  | OSI modelining uchinchi sathi qanday nomlanadi | Tarmoq sathi |
|  | OSI modelining oltinchi sathi qanday nomlanadi | Taqdimlash sathi |
|  | OSI modelining ettinchi sathi qanday nomlanadi | Amaliy sath |
|  | OSI modelining qaysi sathlari tarmoqqa bog’liq sathlar hisoblanadi | fizik, kanal va tarmoq sathlari |
|  | OSI modelining tarmoq sathi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi | Marshrutizator |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi | Fizik sath |
|  | Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi sathi bajaradi | Tarmoq sathi |
|  | Keltirilgan protokollarning qaysilari tarmoq sathi protokollariga mansub | IP, IPX |
|  | Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub | TCP,UDP |
|  | OSI modelining fizik sathi qanday funktsiyalarni bajaradi | Elektr signallarini uzatish va qabul qilish |
|  | OSI modeliningamaliy sathi qanday funktsiyalarni bajaradi | Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | Keltirilgan protokollarning qaysilari kanal sathi protokollariga mansub | Ethernet, FDDI |
|  | Keltirilgan protokollarning qaysilari taqdimlash sathi protokollariga mansub | SNMP, Telnet |
|  | Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu... | Avtorizatsiya |
|  | Autentifikatsiya faktorlari nechta | 3 |
|  | Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima | Parol |
|  | Ko‘z pardasi, yuz tuzilishi, ovoz tembri. | Biometrik autentifikatsiya |
|  | barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi. | Fizik satx |
|  | Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi | 2 |
|  | Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi. | Foydalanishni boshqarish |
|  | Foydalanishni boshqarish –bu... | sub’ektni sub’ektga ishlash qobilyatini aniqlashdir. |
|  | Foydalanishna boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi, | Sub’ekt |
|  | Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ? | Ob’ekt |
|  | Foydalanishna boshqarishning nechta usuli mavjud? | 4 |
|  | Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy ob’ektlarni himoyalash uchun qo‘llaniladi | DAC |
|  | Foydalanishni boshqarishning qaysi modelida ob’ekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi | DAC |
|  | Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi. | MAC |
|  | Foydalanishni boshqarishning mandatli modelida Ob’ektning xavfsizlik darajasi nimaga bog‘liq.. | Tashkilotda ob’ektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi |
|  | MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi | xavfsizlik siyosati ma’muri |
|  | Agar sub’ektning xavfsizlik darajasida ob’ektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi | O‘qish |
|  | Agar sub’ektning xavfsizlik darajasi ob’ektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi. | Yozish |
|  | Foydalanishni boshqarishning qaysi modelida har bir ob’ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun ob’ektlardan foydalanish ruxsati ko‘rsatiladi? | RBAC |
|  | Rol tushunchasiga ta’rif bering. | Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin |
|  | Foydalanishni boshqarishning qaysi usuli - ob’ektlar va sub’ektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. | ABAC |
|  | XACML foydalanishni boshqarishni qaysi usulining standarti? | ABAC |
|  | Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan? | barchasi |
|  | Axborotning kriptografik himoya vositalari necha turda? | 3 |
|  | Dasturiy shifrlash vositalari necha turga bo‘linadi | 4 |
|  | Diskni shifrlash nima uchun amalga oshiriladi? | Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi |
|  | Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi? | 4 |
|  | Kompyuter tarmoqlari bu – | Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi |
|  | Tarmoq modeli –bu.. ikki | Hisoblash tizimlariorasidagi aloqani ularning ichki tuzilmaviy vatexnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir to‘plami |
|  | OSI modelida nechta tarmoq sathi bor | 7 |
|  | OSI modeli 7 stahi bu | Ilova |
|  | OSI modeli 1 stahi bu | Fizik |
|  | OSI modeli 2 stahi bu | Kanal |
|  | TCP/IP modelida nechta satx mavjud | 4 |
|  | Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi. | Shaxsiy tarmoq |
|  | Tarmoq kartasi bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Switch bu... | Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi |
|  | Hab bu... | ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. |
|  | Tarmoq repiteri bu... | Signalni tiklash yoki qaytarish uchun foydalaniladi. |
|  | Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi. | DNS tizimlari |
|  | ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. | TCP |
|  | …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi. | UDP |
|  | Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi. | IP |
|  | Tarmoq taxdidlari necha turga bo‘linadi | 4 |
|  | Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; | Razvedka hujumlari |
|  | Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi | Kirish hujumlari |
|  | Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi; | Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari |
|  | Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi; | Zararli hujumlar |
|  | Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? | Imzo qo‘yish va imzoni tekshirishdan |
|  | Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? | Imzo muallifining ochiq *kaliti yordamida* |
|  | Tarmoq modeli-bu... | Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir |
|  | OSI modeli nechta sathga ajraladi? | 7 |
|  | Fizik sathning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | Ilova sathning vazifasi nimadan iborat | Ilovalarni tarmoqqa ulanish jarayoni |
|  | Kanal sathning vazifasi nimadan iborat | Fizik manzillash |
|  | Tarmoq sathning vazifasi nimadan iborat | Yo‘lni aniqlash va mantiqiy manzillash |
|  | TCP/IP modeli nechta sathdan iborat | 4 |
|  | Quyidagilarninf qaysi biri Kanal sathi protokollari | Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri tarmoq sathi protokollari | . IP, ICMP, ARP, RARP |
|  | Quyidagilarninf qaysi biri transport sathi protokollari | TCP, UDP, RTP |
|  | Quyidagilarninf qaysi biri ilova sathi protokollari | HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP va hak |
|  | TCP/IP modelining kanal sathiga OSI modelining qaysi sathlari mos keladi | Kanal, Fizik |
|  | TCP/IP modelining tarmoq sathiga OSI modelining qaysi sathlari mos keladi | Tarmoq |
|  | TCP/IP modelining transport sathiga OSI modelining qaysi sathlari mos keladi | Tramsport |
|  | TCP/IP modelining ilova sathiga OSI modelining qaysi sathlari mos keladi | Ilova, taqdimot, seans |
|  | Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang. | . Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi. |
|  | Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang. | Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi |
|  | Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang. | Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi |
|  | Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan | Tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi |
|  | Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan | Yuboriluvchi va qabul qilinuvchi ma’lumot TOKYeN yordamida manziliga yetkaziladi |
|  | Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan | Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi |
|  | Tarmoq kartasi nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Repetir nima? | Odatda signalni tiklash yoki qaytarish uchun foydalaniladi |
|  | Hub nima? | Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi |
|  | Switch nima? | Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi |
|  | Router nima? | Qabul qilingan ma’lumotlarni tarmoq sathiga tegishli manzillarga ko‘ra (IP manzil) uzatadi |
|  | DNS tizimlari. | Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi |
|  | TCP bu- … | Transmission Control Protocol |
|  | UDP bu-… | User datagram protocol |
|  | Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang | Ichki, tashqi |
|  | Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi | Biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi | Hujum natijasida ishlab chiqarishi yo‘qolgan hollarda uni qayta tiklash ko‘p vaqt talab qiladi va bu vaqtda ishlab chiqarish to‘xtab qoladi |
|  | Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi | Konfidensial axborotni chiqib ketishi natijasida, tashkilot shaxsiy ma’lumotlarini yo‘qolishi mumkin |
|  | Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi | Tashkilot xodimlarining shaxsiy va ishga oid ma’ulmotlarini kutilmaganda oshkor bo‘lishi ushbu xodimlarga bevosita ta’sir qiladi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi | tizim xizmatlarini xavfsiz bo‘lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto‘g‘ri boshqarilishi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. | Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto‘g‘ri ishlab chiqilgani sabab bo‘ladi. |
|  | Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi | Razvedka hujumlari |
|  | Ma’lumotlarni zaxira nusxalash bu – … | Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi |
|  | Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz | Zaxira nusxalash |
|  | Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering | Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi? | 5 |
|  | Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. | 4 |
|  | Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash | Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | RAID texnologiyasining transkripsiyasi qanday. | Random Array of Independent Disks |
|  | RAID texnologiyasida nechta satx mavjud | 6 |
|  | OSI modelining birinchi sathi qanday nomlanadi | Fizik sath |
|  | OSI modelining ikkinchi sathi qanday nomlanadi | Kanal sathi |
|  | OSI modelining uchinchi sathi qanday nomlanadi | Tarmoq sathi |
|  | OSI modelining oltinchi sathi qanday nomlanadi | Taqdimlash sathi |
|  | OSI modelining ettinchi sathi qanday nomlanadi | Amaliy sath |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi | Fizik sath |
|  | Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub | TCP,UDP |
|  | OSI modelining fizik sathi qanday funktsiyalarni bajaradi | Elektr signallarini uzatish va qabul qilish |
|  | OSI modelining amaliy sathi qanday funktsiyalarni bajaradi | Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | 12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan sonlar soni nechta? | 8 ta |
|  | Yevklid algoritmi qanday natijani beradi? | Sonning eng katta umumiy bo’luvchisini toppish |
|  | Qanday sonlar tub sonlar deb yuritiladi? | Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi. |
|  | To‘liq zaxiralash | To‘liq va o‘sib boruvchi usullarning mujassamlashgan ko‘rinishi bo‘lib, oxirgi zaxiralangan nusxadan boshlab bo‘lgan o‘zgarishlarni zaxira nusxalab boradi. • Amalga oshirish to‘liq zaxiralashga qaraganda tez amalga oshiriladi. • Qayta tiklash o‘sib boruvchi zaxiralashga qaraganda tez amalga oshiriladi. • Ma’lumotni saqlash uchun to‘liq zaxiralashga qaraganda kam joy talab etadi |
|  | O‘sib boruvchi zaxiralash | Zaxiralangan ma’lumotga nisbatan o‘zgarish yuz berganda zaxirilash amalga oshiriladi. • Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usuli bo‘lishi mumkin (to‘liq saxiralashdan). • Saqlash uchun kam hajm va amalga oshirish jarayoni tez |
|  | Differensial zaxiralash | Ushbu zaxiralashda tarmoqga bog‘lanishamalga oshiriladi. • Iliq zaxiralashda, tizim yangilanishi davomiy yangilanishni qabul qilish uchun ulanadi |
|  | Ushbu jarayon ma’lumot qanday yo‘qolgani, ma’lumotni qayta tiklash dasturiy vositasi va ma’lumotni tiklash manzilini qayergaligiga bog‘liq bo‘ladi. Qaysi jarayon | Ma’lumotlarni qayta tiklash |
|  | Antivirus dasturlarini ko’rsating? | Drweb, Nod32, Kaspersky |
|  | Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi | wep, wpa, wpa2 |
|  | Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak? | ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | bit |
|  | Virtual xususiy tarmoq – bu? | VPN |
|  | Xavfli viruslar bu - … | kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Rezident virus... | tezkor xotirada saqlanadi |
|  | DIR viruslari nimani zararlaydi? | FAT tarkibini zararlaydi |
|  | .... kompyuter tarmoqlari bo’yicha tarqalib, komlg’yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi | «Chuvalchang» va replikatorli virus |
|  | Mutant virus... | shifrlash va deshifrlash algoritmlaridan iborat- to’g’ri javob |
|  | Fire Wall ning vazifasi... | tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi |
|  | Kompyuter virusi nima? | maxsus yozilgan va zararli dastur |
|  | Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating | disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali |
|  | Troyan dasturlari bu... | virus dasturlar |
|  | Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? | 5 |
|  | Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud | detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya mahnosi... | sirli yozuv |
|  | …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi | K.Shennon |
|  | Kriptologiya yo’nalishlari nechta? | 2 |
|  | Kriptografiyaning asosiy maqsadi... | maxfiylik, yaxlitlilikni ta`minlash |
|  | Zararli dasturiy vositalarni aniqlash turlari nechta | 3 |
|  | Signaiurana asoslangan | ...bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
|  | O‘zgarishni aniqlashga asoslangan | Zararli dasturlar biror joyda joylashishi sababli, agar tizimdagi biror joyga o‘zgarishni aniqlansa, u holda u zararlanishni ko‘rsatishi mumkin |
|  | Anomaliyaga asoslangan | Noodatiy yoki virusga o‘xshash yoki potensial zararli harakatlari yoki xususiyatlarni topishni maqsad qiladi |
|  | Antiairuslar qanday usulda viruslarni aniqlaydi | Signaturaga asoslangan |
|  | Viruslar - | o‘zini o‘zi ko‘paytiradigan programma bo‘lib, o‘zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi |
|  | Rootkitlar- | ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi |
|  | Backdoorlar - | zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish |
|  | Troyan otlari- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Ransomware- | mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo‘yib, to‘lov amalga oshirilishini talab qiladi |
|  | Resurslardan foydalanish usuliga ko’ra viruslar qanday turlarga bo’linadi | Virus parazit, Virus cherv |
|  | Zararlagan obyektlar turiga ko’ra | Dasturiy, yuklanuvchi, Makroviruslar, multiplatformali viruslar |
|  | Faollashish prinspiga ko’ra | Resident, Norezident |
|  | Dastur kodini tashkil qilish yondashuviga ko‘ra | Shifrlangan, shifrlanmagan, Polimorf |
|  | Shifrlanmagan viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang | 840 |
|  | 256mod25=? | 6 |
|  | bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi. | Tizim |
|  | Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to‘plami nima duyidadi | Xavfsizlik siyosati |
|  | RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday? | *p* va *q* –sonlarning ko‘paytmasini ifodalovchi sonning spektoriga teng; |
|  | DES algoritmi akslantirishlari raundlari soni qancha? | 16; |
|  | DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha? | CHap qism blok 32 bit, o‘ng qism blok 32 bit; |
|  | Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? | SHifrlash va deshifrlash jarayonlari uchun kalitlarni generatsiya qilish qoidalariga ko‘ra farqlanadi |
|  | 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta? | 18 ta |
|  | 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta? | 4 ta |
|  | Eyler funsiyasida 𝜙(1) qiymati nimaga teng? | 0 |
|  | Eyler funksiyasida 60 sonining qiymatini toping. | 59 |
|  | Eyler funksiyasi yordamida 1811 sonining qiymatini toping. | 1810 |
|  | 97 tub sonmi? | Tub |
|  | Quyidagi modulli ifodani qiymatini toping (148 + 14432) mod 256. | 244 |
|  | Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220 | 44 |
|  | Quyidagi ifodani qiymatini toping. -17mod11 | 5 |
|  | 2 soniga 10 modul bo’yicha teskari sonni toping. | Ø |
|  | Tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta’minlash sohasidagi tadbirlar tavsiflanadigan yuqori darajadagi reja nima? | Kiberxavfsizlik siyosati |
|  | Kiberxavfsizlik siyosati tashkilotda nimani ta’minlaydi? | tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta’minlaydi |
|  | Kiberxavfsizlikni ta’minlash masalalari bo’yicha xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang | SANS (System Administration Networking and Security) |
|  | Korxonaning davomli muvaffaqiyat bilan faoliyat yuritishinita’minlashga mo’ljallangan strukturalangan va o’zaro bog’langan harakatlar to’plami- … | Strategiya |
|  | Tahdidlarning muvaffaqiyatli amalga oshirilishiga imkon beruvchi har qanday omil – bu … | Zaiflik |
|  | ISO/IEC 27002:2005 – …. | Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari |
|  | O’zDStISO/IEC 27005:2013 – …. | Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish |
|  | Axborot xavfsizligi arxitekturasining nechta satxi bor? | 3 |
|  | Rahbariy hujjat. Ma’lumotlar uzatish tarmog’ida axborot xavfsizligini ta’minlash to’g’risida Nizom - Xujjat raqamini toping | RH 45-215:2009 |
|  | Davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta’minlash dasturini ishlab chiqish tartibi - Xujjat raqamini toping | RH 45-185:2011 |
|  | Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta’minlash darajasini aniqlash tartibi - Xujjat raqamini toping | RH 45-193:2007 |
|  | Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta’riflar - Xujjat raqamini toping | TSt 45-010:2010 |
|  | Quyidagilardan qaysi standart aloqa va axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta’riflarni belgilaydi? | TSt 45-010:2010 |
|  | Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni nima? | Identifikatsiya |
|  | Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima? | Autentifikatsiya |
|  | Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni – nima deyiladi? | Avtorizatsiya |
|  | Identifikatsiya nima? | Sub’ekt identifikatorini tizimga yoki talab qilgan sub’ektga taqdim qilish jarayoni |
|  | Autentifikatsiya nima? | Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni |
|  | Avtorizatsiya nima? | Identifikatsiya va autentifikatsiyadan o’tgan foydalanuvchilarga tizimda bajarishi mumkin bo’lgan amallarga ruxsat berish jarayoni |
|  | ... - Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o’tishni ta’minlovchi biror axborot | Parol |
|  | Smart karta o’lchamidagi, kichik xajmdagi xotira va xisoblash imkoniyatiga ega bo’lgan, o’zida parol yoki kalitni saqlovchi qurilma nima deb ataladi? | Token, Smartkarta |
|  | Smarkarta nima asosida autentifikatsiyalaydi? | Something you have |
|  | Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o’zgarib turadigan parol nima deyiladi? | One-time password (OTP) |
|  | Foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish nima deb ataladi? | Ma’murlash |
|  | Amaldagi qonunchilikka mos ravishda texnik, dasturiy va dasturiy-texnik vositalar yordamida axborot xavfsizligining nokriptografik usullari bilan ta’minlashni inobatga oluvchi axborot himoyasi nima? | Axborotning texnik himoyasi |
|  | Nazorat hududi – bu ... | Qo’riqlanuvchi soha bo’lib, uning ichida kommunikatsiya qurilmalari hamda axborot tarmog’ining lokal tarkibiy qurilmalarini birlashtiruvchi barcha nuqtalar joylashadi |
|  | Texnik himoya vositalari – bu ... | Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob’ektni himoyalashdir |
|  | Bu axborotni tutib olish qurilmasi bo’lib, ularda uzatuvchi qurilma sifatida kontaktli mikrofonlardan foydalaniladi | Stetoskoplar |
|  | Xesh funktsiya to’g’ri ko’rsatilgan javobni aniqlang. | MD5 |
|  | MD5, SHA1, Tiger xesh funktsiyalari uchun blok uzunligi necha baytga teng? | 64 bayt |
|  | Sub’ektni ob’ektga ishlash qobilyatini aniqlash – nima? | Foydalanishni boshqarish |
|  | Foydalanishni boshqarishda sub’ekt bu - .... | Inson, dastur, jarayon |
|  | Foydalanishni boshqarishning qaysi usuli tizimdagi shaxsiy ob’ektlarni ximoyalash uchun qo’llaniladi? | Discretionary access control DAC |
|  | Foydalanishni boshqarishning qaysi usulidan asosan operatsion tizimlarda qo’llaniladi? | Discretionary access control DAC |
|  | Foydalanishni boshqarishning qaysi usulida foydalanishlar sub’ektlar va ob’ektlarni klassifikatsiyalashga asosan boshqariladi? | Mandatory access control MAC |
|  | Foydalanishni boshqarishning qaysi usulida xavfsizlik markazlashgan tarzda xavfsizlik siyosati m’muri tomonidan amalga oshiriladi? | Mandatory access control MAC |
|  | Foydalanishni boshqarishning qaysi usulida xar bir foydalanuvchini foydalanish ruxsatini belgilash o’rniga rol uchun ob’ektlardan foydalanish ruxsatini ko’rsatish yetarli bo’ladi? | Role-based access control RBAC |
|  | Foydalanishni boshqarishning qaysi usulida sub’ekt va ob’ektlarga tegishli xuquqlarni ma’murlash oson kechadi? | Role-based access control RBAC |
|  | Firibgarlikni oldini olish uchun bir shaxs tomonidan ko’plab vazifalarni bajarishga ruxsat bermaslik zarur. Bu muammo foydalanishni boshqarishni qaysi usulida bartaraf etiladi? | Role-based access control RBAC |
|  | Ob’ekt va sub’ektlarning attributlari, ular bilan mumkin bo’lgan amallar va so’rovlarga mos keladigan muxit uchun qoidalarni taxlil qilish asosida foydalanishni boshqarish - .... | Attribute based access control ABAC |
|  | Attribute based access control ABAC usuli attributlari qaysilar? | Foydalanuvchi attributlari, Resurs attributlari, Ob’ekt va muxit attributlari |
|  | Foydalanishni boshqarishning qaysi usulida ruxsatlar va xarakatni kim bajarayotganligi to’g’risidagi xolatlar “agar, u xolda” buyrug’idan tashkil topgan qoidalarga asoslanadi? | Attribute based access control ABAC |
|  | XASML standarti foydalanishni boshqarishning qaysi usulida qo’llaniladi? | Attribute based access control ABAC |
|  | XASML standartida qoida nima? | Maqsad, ta’sir, shart, majburiyat va maslaxatlar |
|  | XASML standartida maqsad nima? | Sub’ekt ob’ekt ustida nima xarakat qilishi |
|  | Lampsonning foydalanishni boshqarish matritsasi nimalardan tashkil topgan? | Imtiyozlar ro’yxati |
|  | Access control list va Capability list bu nimaning asosiy elementi xisoblanadi? | Lampson matritsasining |
|  | Lampson matritsasining satrlarida nima ifodalanadi? | Sub’ektlar |
|  | Foydalanishni boshqarishning mantiqiy vositalari infratuzilma va uning ichidagi tizimlarda ... uchun foydalaniladi. | Mandat, Tasdiqlash, Avtorizatsiya |
|  | SHaxsiy simsiz tarmoq standartini aniqlang. | Bluetooth, IEEE 802.15, IRDA |
|  | Lokal simsiz tarmoq standartini aniqlang. | IEEE 802.11, Wi-Fi, HiperLAN |
|  | Regional simsiz tarmoq standartini aniqlang. | IEEE 802.16, WiMAX |
|  | Global simsiz tarmoq standartini aniqlang. | CDPD, 2G, 2.5G, 3G, 4G, 5G |
|  | Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang. | SHaxsiy simsiz tarmoq |
|  | IEEE 802.11, Wi-Fi, HiperLAN standartida ishlovchi simsiz tarmoq turini aniqlang. | Lokal simsiz tarmoq |
|  | IEEE 802.16, WiMAX standartida ishlovchi simsiz tarmoq turini aniqlang. | Regional simsiz tarmoq |
|  | CDPD, 2G, 2.5G, 3G, 4G, 5G standartida ishlovchi simsiz tarmoq turini aniqlang. | Global simsiz tarmoq |
|  | Bluetooth qanday chastota oralig’ida ishlaydi? | 2.4-2.485 Ggts |
|  | Wi-Fi qanday chastota oralig’ida ishlaydi? | 2.4-5 Ggts |
|  | WiMax tarmog’ining tezligi qancha? | 1 Gbit/sekund |
|  | Quyidagilardan qaysi biri MITM xujumiga tegishli xatti-xarakat ximoblanadi? | Aloqa seansini konfidentsialligini va yaxlitligini buzish |
|  | WiMAX tarmoq arxitekturasi nechta tashkil etuvchidan iborat? | 5 |
|  | WiMAX tarmoq arxitekturasi qaysi tashkil etuvchidan iborat? | Base station, Subscriber station, Mobile station, Relay station, Operator network |
|  | GSM raqamli mobil telefonlarining nechanchi avlodi uchun ishlab chiqilgan protokol? | Ikkinchi avlodi |
|  | GSM standarti qaysi tashkilot tomonidan ishlab chiqilgan? | European telecommunications standards institute |
|  | .... – o’zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma’lumoti va xavfsizlik algoritmlarini saqlaydi. | Sim karta |
|  | Rutoken S qurilmasining og’irligi qancha? | 6.3 gramm |
|  | True Crypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES, Serpent, Twofish |
|  | Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidentsialligini aniqlash qaysi dasturiy shifrlash vositalarining vazifasi? | Disc encryption software |
|  | BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES, Serpent, Twofish |
|  | AxCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? | AES-256 |
|  | Qog’oz ko’rinishidagi axborotlarni yo’q qilish qurilmasining nomini kiriting. | Shreder |
|  | Ma’lumotlarni bloklarga bo’lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya? | RAID 0 |
|  | Qaysi texnologiyada ma’lumotni ko’plab nusxalari bir vaqtda bir necha disklarga yoziladi? | RAID 1 |
|  | Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi? | RAID 3 |
|  | Qaysi texnologiyada ma’lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi? | RAID 5 |
|  | Disk zararlanganda “qaynoq almashtirish” yordamida uni almashtirish mumkin. Bu xususiyat qaysi texnologiyaga tegishli? | RAID 50 |
|  | Zaxiralashning qanday turlari mavjud? | To’liq, o’sib boruvchi, differentsial |
|  | IOS, Android, USB xotiralardan ma’lumotlarni tiklash uchun qaysi dasturdan foydalaniladi? | EASEUS Data recovery wizard |
|  | Foydalanuvchi ma’lumotlarini qo’lga kirituvchi va uni xujumchiga yuboruvchi dasturiy kod nima? | Spyware |
|  | Operatsion tizim tomonidan aniqlanmasligi uchun ma’lum xarakatlarni yashirish nima deyiladi? | Rootkits |
|  | Qurbon kompyuterda mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo’yib to’lov amalga oshirishni talab qiladi. Bu qaysi zararli dastur? | Ransomware |
|  | Quyidagilardan o’zidan ko’payishi yo’q bo’lganlarini belgilang. | Mantiqiy bomba, Troyan oti, Backdoors |
|  | Viruslar resurslardan foydalanish usuliga ko’ra qanday turlarga bo’linadi? | Virus parazitlar, virus chervlar |
|  | Viruslar zararlangan ob’ektlar turiga ko’ra qanday turlarga bo’linadi? | Dasturiy, yuklanuvchi, makroviruslar, ko’p platformali |
|  | Viruslar faollashish printsipiga ko’ra qanday turlarga bo’linadi? | Rezident, norezident |
|  | Viruslar dastur kodini tashkil qilish yondoshuviga ko’ra qanday turlarga bo’linadi? | SHifrlangan, shifrlanmagan, polimorf |
|  | Dastlabki virus nechanchi yilda yaratilgan? | 1988 |
|  | ILOVEYOU virusi keltirgan zarar qancha? | 10 mlrd. Dollar |
|  | CodeRed virusi keltirgan zarar qancha? | 2 mlrd. Dollar |
|  | Melissa virusi keltirgan zarar qancha? | 80 million dollar |
|  | NetSky virusi keltirgan zarar qancha? | 18 mlrd. Dollar |
|  | MyDoom virusi keltirgan zarar qancha? | 38 mlrd. Dollar |
|  | Risk monitoring ….. ni paydo bo’lish imkoniyatini aniqlaydi. | Yangi risklar |
|  | ….. riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi. | Risk monitoring |
|  | Axborot xavfsizligi siyoatining necha hil turi bor? | 3 |
|  | Internetdan foydalanish siyosatining nechta turi mavjud? | 4 |
|  | Nomuntazam siyosat (Promiscuous Policy) nima? | Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi |
|  | Paranoid siyosati (Paranoid Policy) – bu …. | Hamma narsa ta’qiqlanadi |
|  | Ruxsat berishga asoslangan siyosat (Permissive Policy) – bu … | Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi |
|  | Ehtiyotkorlik siyosati (Prudent Policy) – bu …. | Barcha hizmatlar blokirovka qilingandan so’ng bog’lanadi |
|  | Tizim resurslaridan foydalanishda hech qanday cheklovlar qo’ymaydi. Bu qaysi xavfsizlik siyosatiga hos? | Nomuntazam siyosat (Promiscuous Policy) |
|  | Barcha hizmatlar blokirovka qilingandan so’ng bog’lanadi. Bu qaysi xavfsizlik siyosatiga hos? | Ehtiyotkorlik siyosati (Prudent Policy) |
|  | Faqat ma’lum hizmatlar/hujumlar/harakatlar bloklanadi. Bu qaysi xavfsizlik siyosatiga hos? | Ruxsat berishga asoslangan siyosat (Permissive Policy) |
|  | Hamma narsa ta’qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos? | Paranoid siyosati (Paranoid Policy) |
|  | Tizim arxitekturasining turlari nechta? | 5 |
|  | Internet, havo hujumidan mudofaa, transport tizimlari qaysi tizim arxitekturasiga xos? | Hamkorlik tizimlari arxitekturasi |
|  | Cloud computing texnologiyasining nechta asosiy turi mavjud? | 3 |
|  | Raqamli soatlar qaysi texnologiyaga tegishli? | O’rnatilgan tizimlar (Embedde systems) |
|  | Xavfsizlikning asosiy yo’nalishlarini sanab o’ting. | \*Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik |
|  | Axborot xavfsizligining asosiy maqsadlaridan biri- bu… | \*Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish |
|  | Konfidentsiallikga to’g’ri ta`rif keltiring. | \*axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; |
|  | Yaxlitlikni buzilishi bu - … | \*Soxtalashtirish va o’zgartirish |
|  | ... axborotni himoyalash tizimi deyiladi. | \*Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo’qotilishiga to’sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi |
|  | Kompyuter virusi nima? | \*maxsus yozilgan va zararli dastur |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | \*kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya ma’nosi... | \*sirli yozuv |
|  | Kriptografiyaning asosiy maqsadi... | \*maxfiylik, yaxlitlilikni ta`minlash |
|  | SMTP - Simple Mail Transfer protokol nima? | \*elektron pochta protokoli |
|  | SKIP protokoli... | \*Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi |
|  | Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar… | \*uzilish, tutib qolish, o’zgartirish, soxtalashtirish |
|  | ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. | \*konfidentsiallik |
|  | Foydalanish huquqini cheklovchi matritsa modeli bu... | \*Bella La-Padulla modeli |
|  | Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? | \*TCP/IP, X.25 protokollar |
|  | Himoya tizimi kompleksligiga nimalar orqali erishiladi? | \*Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali |
|  | Kalit – bu … | \*Matnni shifrlash va shifrini ochish uchun kerakli axborot |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | \*simmetrik kriptotizimlar |
|  | Autentifikatsiya nima? | \*Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi |
|  | Identifikatsiya bu- … | \*Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni |
|  | O’rin almashtirish shifri bu - … | \*Murakkab bo’lmagan kriptografik akslantirish |
|  | Simmetrik kalitli shifrlash tizimi necha turga bo’linadi. | \*2 turga |
|  | Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular … | \*hosil qilish, yig’ish, taqsimlash |
|  | Kriptologiya - | \*axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi |
|  | Kriptografiyada alifbo – | \*axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam |
|  | Simmetrik kriptotizimlarda ... jumlani davom ettiring | \*shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi |
|  | Kriptobardoshlilik deb … | \*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Elektron raqamli imzo deb – | \*xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha |
|  | Kriptografiya – | \*axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi |
|  | Kriptografiyada matn – | \*alifbo elementlarining tartiblangan to’plami |
|  | Kriptoanaliz – | \*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi |
|  | Shifrlash – | \*akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi |
|  | Kalit taqsimlashda ko’proq nimalarga e`tibor beriladi? | \*Tez, aniq va maxfiyligiga |
|  | Faol hujum turi deb… | \*Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon |
|  | Blokli shifrlash- | \*shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish |
|  | Simmetrik kriptotizmning uzluksiz tizimida … | \*ochiq matnning har bir harfi va simvoli alohida shifrlanadi |
|  | Kripto tizimga qo’yiladigan umumiy talablardan biri | \*shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak |
|  | 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 |
|  | Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang | \*Vijener matritsasi, Sezar usuli |
|  | Akslantirish tushunchasi deb nimaga aytiladi? | \*1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga |
|  | Simmetrik guruh deb nimaga aytiladi? | \*O’rin almashtirish va joylashtirish |
|  | Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq? | \*simmetrik kriptosistemalar |
|  | Xavfli viruslar bu - … | \*kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | \*Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi? | \*raqamli imzoni shakllantirish va tekshirish muolajasi |
|  | Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? | \*Simmetrik va assimetrik |
|  | Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin? | \*Korporativ va umumfoydalanuvchi |
|  | Elektromagnit nurlanish va ta`sirlanishlardan himoyalanish usullari nechta turga bo’linadi? | \*Sust va faol |
|  | Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? | \*SMTP, POP yoki IMAR |
|  | Axborot resursi – bu? | \*axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi |
|  | Shaxsning, o’zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo’llaniladigan belgilar ketma-ketligi bo’lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo’lish uchun foydalaniluvchining maxfiy bo’lmagan qayd yozuvi – bu? | \*login |
|  | Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu? | \*parol |
|  | Identifikatsiya jarayoni qanday jarayon? | \* axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni |
|  | Autentifikatsiya jarayoni qanday jarayon? | \*obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash |
|  | Avtorizatsiya jarayoni qanday jarayon? | \*foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni |
|  | Ro’yxatdan o’tish bu? | \*foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni |
|  | Axborot qanday sifatlarga ega bo’lishi kerak? | \*ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | \*bit |
|  | Elektron hujjatning rekvizitlari nechta qismdan iborat? | \*4 |
|  | Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? | \*fleshka, CD va DVD disklar |
|  | Imzo bu nima ? | \*hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati. |
|  | Muhr bu nima? | \*hujjatning haqiqiyligini va biror bir yuridik shaxsga tegishli ekanligini tasdiqlovchi isbotdir |
|  | DSA – nima | \*Raqamli imzo algoritmi |
|  | El Gamal algoritmi qanday algoritm | \*Shifrlash algoritmi va raqamli imzo algoritmi |
|  | Sezarning shifrlash sistemasining kamchiligi | \*Harflarning so’zlarda kelish chastotasini yashirmaydi |
|  | Axborot xavfsizligi va xavfsizlik san’ati haqidagi fan …. deyiladi? | \*Kriptografiya |
|  | Tekstni boshqa tekst ichida ma’nosini yashirib keltirish bu - | \*steganografiya |
|  | Shifrtekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? | \*Deshifrlash |
|  | …… – hisoblashga asoslangan bilim sohasi bo‘lib,  buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. | \*Kiberxavfsizlik |
|  | Risk | \*Potensial foyda yoki zarar |
|  | Tahdid nima? | \*Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
|  | Kodlash nima? | \*Ma’lumotni osongina qaytarish uchun hammaga  ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir |
|  | Shifrlash nima? | Ma’lumotni osongina qaytarish uchun hammaga  ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir |
|  | Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi | Kriptoanaliz |
|  | Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi | {*d, e*} – ochiq, {*e, n*} – yopiq; |
|  | Zamonaviy kriptografiya qanday bo’limlardan iborat? | Electron raqamli imzo; kalitlarni boshqarish |
|  | Kriptografik usullardan foydalanishning asosiy yo’nalishlari nimalardan iborat? | uzatiliyotgan xabarlarni haqiqiyligini aniqlash |
|  | Shifr nima? | \* Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm |
|  | Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? | \*Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi |
|  | Oqimli shifrlashning mohiyati nimada? | Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,  Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi |
|  | Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating. | \*uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo’lmasligi uchun algoritm yetarli darajada bardoshli bo’lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog’liq bo’lishi lozim, |
|  | Kriptotizim qaysi komponentlardan iborat? | \*ochiq matnlar fazosi M, Kalitlar fazosi K,  Shifrmatnlar fazosi C, Ek : M → C (shifrlash uchun) va Dk: C→M (deshifrlash uchun) funktsiyalar |
|  | Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? | \*shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun |
|  | Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi. | \*ochiq kalitlar |
|  | Xesh-funktsiyani natijasi … | Kiruvchi xabar uzunligidan uzun xabar |
|  | RSA algoritmi qanday jarayonlardan tashkil topgan | \*Kalitni generatsiyalash; Shifrlash; Deshifrlash. |
|  | Ma’lumotlar butunligi qanday algritmlar orqali amalga oshiriladi | \*Xesh funksiyalar |
|  | To’rtta bir-biri bilan bog’langan bog’lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub | \*Xalqa |
|  | Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo’llamasligi mumkin? | \*to’liq bog’lanishli |
|  | Kompyuterning tashqi interfeysi deganda nima tushuniladi? | \*kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari |
|  | Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? | \*Yulduz |
|  | Ethernet kontsentratori qanday vazifani bajaradi | \*kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi |
|  | OSI modelida nechta satx mavjud | \*7 |
|  | OSI modelining to’rtinchi satxi qanday nomlanadi | \*Transport satxi |
|  | OSI modelining beshinchi satxi qanday nomlanadi | \*Seanslar satxi |
|  | OSI modelining birinchi satxi qanday nomlanadi | \*Fizik satx |
|  | OSI modelining ikkinchi satxi qanday nomlanadi | \*Kanal satxi |
|  | OSI modelining uchinchi satxi qanday nomlanadi | \*Tarmoq satxi |
|  | OSI modelining oltinchi satxi qanday nomlanadi | \*Taqdimlash satxi |
|  | OSI modelining yettinchi satxi qanday nomlanadi | \*Amaliy satx |
|  | OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi | \*fizik, kanal va tarmoq satxlari |
|  | OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi | \*Marshrutizator |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi | \*Fizik satx |
|  | Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi | \*Tarmoq satxi |
|  | Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub | \*IP, IPX |
|  | Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub | \*TCP,UDP |
|  | OSI modelining fizik satxi qanday funktsiyalarni bajaradi | \*Elektr signallarini uzatish va qabul qilish |
|  | OSI modelining amaliy satxi qanday funktsiyalarni bajaradi | \*Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub | \*Ethernet, FDDI |
|  | Keltirilgan protokollarning qaysilari taqdimlash satxi protokollariga mansub | \*SNMP, Telnet |
|  | Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu... | \*Avtorizatsiya |
|  | Autentifikatsiya faktorlari nechta | 4 |
|  | Faqat foydalanuvchiga ma’lum va biror tizimda autentifikatsiya jarayonidan o‘tishni ta’minlovchi biror axborot nima | Login |
|  | Ko‘z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar? | Biron nimaga egalik asosida |
|  | barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi? | \*Fizik satx |
|  | Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi | \*2 |
|  | Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? | \*Foydalanishni boshqarish |
|  | Foydalanishni boshqarish –bu... | Subyektni Subyektga ishlash qobilyatini aniqlashdir. |
|  | Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi? | Obyekt |
|  | Foydalanishna boshqarishda ma’lumot , resurs, jarayon nima vazifani bajaradi ? | \*Obyekt |
|  | Foydalanishna boshqarishning nechta usuli mavjud? | \*4 |
|  | Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo‘llaniladi | ABAC |
|  | Foydalanishni boshqarishning qaysi modelida Obyekt egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi | ABAC |
|  | Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi. | ABAC |
|  | Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bog‘liq.. | Tashkilotda Obyektning muhimlik darajasi bilan yoki yuzaga keladigan foyda miqdori bilan bilan xarakterlanadi |
|  | MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi | \*xavfsizlik siyosati ma’muri |
|  | Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi | Yozish |
|  | Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi. | \*Yozish |
|  | Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun Obyektlardan foydalanish ruxsati ko‘rsatiladi? | ABAC |
|  | Rol tushunchasiga ta’rif bering. | \*Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin |
|  | 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 |
|  | XACML foydalanishni boshqarishni qaysi usulining standarti? | \*ABAC |
|  | Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan? | \*barchasi |
|  | Axborotning kriptografik himoya vositalari necha turda? | 4 |
|  | Dasturiy shifrlash vositalari necha turga bo‘linadi | \*4 |
|  | Diskni shifrlash nima uchun amalga oshiriladi? | \*Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi |
|  | Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi? | 8 |
|  | Kompyuter tarmoqlari bu – | \*Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi |
|  | Tarmoq modeli –bu.. ikki | Matematik modellar to‘plami |
|  | OSI modelida nechta tarmoq satxi bor | \*7 |
|  | OSI modeli 7 satxi bu | \*Ilova |
|  | OSI modeli 1 satxi bu | Ilova |
|  | OSI modeli 2 satxi bu | Ilova |
|  | TCP/IP modelida nechta satx mavjud | \*4 |
|  | Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi? | Lokal |
|  | Tarmoq kartasi bu... | \*Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Switch bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Hab bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Tarmoq repiteri bu... | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. |
|  | Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi. | \*DNS tizimlari |
|  | ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. | \*TCP |
|  | …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi. | \*UDP |
|  | Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi. | TCP |
|  | Tarmoq taxdidlari necha turga bo‘linadi | 2 |
|  | Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; | \*Razvedka hujumlari |
|  | Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi | Razvedka hujumlari |
|  | Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi; | Razvedka hujumlari |
|  | Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi; | Razvedka hujumlari |
|  | RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart? | \*e soni Eyler funksiyasi -bilan o‘zaro tub |
|  | RSA elektron raqamli imzo algoritmidagi yopiq kalit  d qanday hisoblanadi? Bu yerda p va q tub sonlar,n=pq,- Eyler funksiyasi,e-ochiq kalit | \* |
|  | Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi? | \*Imzo qo‘yish va imzoni tekshirishdan |
|  | Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? | \*Imzo muallifining ochiq *kaliti yordamida* |
|  | Tarmoq modeli-bu... | \*Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir |
|  | OSI modeli nechta satxga ajraladi? | 2 |
|  | Fizik satxning vazifasi nimadan iborat | \*Qurilma, signal va binar o‘zgartirishlar |
|  | Ilova satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | Kanal satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | Tarmoq satxning vazifasi nimadan iborat | Qurilma, signal va binar o‘zgartirishlar |
|  | TCP/IP modeli nechta satxdan iborat | \*4 |
|  | Quyidagilarninf qaysi biri Kanal satxi protokollari | \*Ethernet, Token Ring, FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri tarmoq satxi protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri transport satxi protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | Quyidagilarninf qaysi biri ilova satxi protokollari | Ethernet, Token Ring,FDDI, X.25, Frame  Relay, RS-232, v.35. |
|  | TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi | \*Kanal, Fizik |
|  | TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi | Kanal, Fizik |
|  | TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi | Kanal, Fizik |
|  | TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos keladi | Kanal, Fizik |
|  | Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang. | \*Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan MAN tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni belgilang. | Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. |
|  | Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan | \*Tarmoqda har bir kompyuter yoki tugun Markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan | Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi |
|  | Tarmoq kartasi nima? | \*Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Repetir nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Hub nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Switch nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | Router nima? | Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi |
|  | DNS tizimlari. | \*Host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi |
|  | TCP bu- … | \*Transmission Control Protocol |
|  | UDP bu-… | User domain protocol |
|  | IP protokolining necha xil versiyasi mavjud? | 1 |
|  | Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang | \*Ichki, tashqi |
|  | Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi | \*Biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo’qolishi qanday oqibatlarga olib keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo’qolishi qanday oqibatlarga olib keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Tarmoq xavfsizligining buzilishi natijasida axborotning o’g’irlanishi qanday oqibatlarga olib keladi | Biznesda ixtiyoriy hujum biznes jarayonlarni to‘xtab qolishiga olib keladi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi | \*Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya  usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya  usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Quyidagi ta’riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. | Tarmoq qurilmalari, svitch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo‘lmasligi |
|  | Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi | \*Razvedka hujumlari |
|  | Razvedka hujumiga berilgan ta’rifni aniqlang | \*Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
|  | Kirish hujumiga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axboro ni to‘plashni maqsad qiladi; |
|  | DOS hujumiga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
|  | Zararli hujumga berilgan ta’rifni aniqlang | asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi; |
|  | Razvetka hujumari necha turga bo’linadi | 1 |
|  | Qaysi hujum jarayoni TCP/IP tarmog‘ida paketlarni tutib  olish, dekodlash, tekshirish va tarjima qilishni o‘z ichiga  oladi | \*Paketlarni snifferlash |
|  | 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 |
|  | 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 |
|  | Tarmoqlaro ekranni bajarilishiga ko’ra qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida |
|  | Tarmoqlaro ekranni ulanish sxemasi bo’yicha qanday turlarga bo’lindi? | paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahidaishlaydi; ilova proksilari – ilova satxida |
|  | Paket filtrlari tarmoqlararo ekrani vazifasi nima? | \*Tarmoq satxida paketlarni  tahlillashga asoslan; |
|  | Ilova proksilari tarmoqlararo ekrani vazifasi nima? | Tarmoq satxida paketlarni tahlillashga asoslan; |
|  | Ekspert paket filtrlari tarmoqlararo ekrani vazifasi nima? | Tarmoq satxida paketlarni tahlillashga asoslan; |
|  | 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. |
|  | 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. |
|  | Simsiz tarmoqlarning nechta turi mavjud | 5 |
|  | Bluetooth qanday simsiz tarmoq turiga kiradi. | Global |
|  | Wifi qanday simsiz tarmoq turiga kiradi. | Global |
|  | LTE, CDMA, HSDPA qanday simsiz tarmoq turiga kiradi. | \*Global |
|  | WiMAX qanday simsiz tarmoq turiga kiradi. | Global |
|  | Bluetooth texnologiyasida autentifikatsiya bu… | Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. |
|  | Bluetooth texnologiyasida konfidensiallik bu… | \*Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. |
|  | Bluetooth texnologiyasida avtorizatsiya bu… | Ikki autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. |
|  | GSM bu ..- | \*Global System for Mobile Communications |
|  | Simsiz tarmoq Bluetooth ishlash rejimlari nechta? | 2 |
|  | Kompyuterda hodisalar haqidagi ma’lumot qayerda saqlanadi? | \*hodisalar jurnaliga |
|  | 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. |
|  | 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. |
|  | 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. |
|  | 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. |
|  | 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. |
|  | Ma’lumotlarni zaxira nusxalash bu – … | \*Muhim bo‘lgan axborot nusxalash yoki saqlash jarayoni bo‘lib, bu ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi |
|  | Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma’lumotni yo‘qolishidan so‘ng uni qayta tiklash uchun qanday amaldan foydalanamiz | \*Zaxira nusxalash |
|  | Ma’lumotlarni inson xatosi tufayli yo’qolish sababiga ta’rif bering | \*Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi. |
|  | 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. |
|  | 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. |
|  | 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. |
|  | Zahira nusxalash strategiyasi nechta bosqichni o’z ichiga oladi? | 7 |
|  | Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. | \*4 |
|  | Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta’rifni nelgilash | \*Har bir tashkilot o‘zining budjetiga mos bo‘lgan zaxira nusxalash vositasiga ega bo‘lishi shart. |
|  | 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. |
|  | 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. |
|  | 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. |
|  | 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. |
|  | RAID texnologiyasining transkripsiyasi qanday. | Redundant Array of Independent Disks |
|  | RAID texnologiyasida nechta satx mavjud | 3 |
|  | 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 |
|  | 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 |
|  | 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 |
|  | 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 |
|  | RAID 10: diskni navbatlanishi bu-.. | \*Gibrid satx bo‘lib, RAID 1 va RAID 0  satxlaridan iborat va kamida 4 ta diskni talab etadi |
|  | RAID 50: diskni navbatlanishi bu-.. | Gibrid satx bo‘lib, RAID 1 va RAID 0  satxlaridan iborat va kamida 4 ta diskni talab etadi |
|  | Ma’lumotlarni nusxalash usullari necha xil usulda amalga oshiriladi? | \*3 |
|  | 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. |
|  | 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. |
|  | 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. |
|  | Ichki zahiralash qanday amalga oshiriladi | Ichki zahiralashda mahalliy yoki global serverlardan foydalaniladi |
|  | OSI modelining birinchi satxi qanday nomlanadi | \*Fizik satx |
|  | OSI modelining ikkinchi satxi qanday nomlanadi | \*Kanal satxi |
|  | OSI modelining uchinchi satxi qanday nomlanadi | \*Tarmoq satxi |
|  | OSI modelining oltinchi satxi qanday nomlanadi | \*Taqdimlash satxi |
|  | OSI modelining ettinchi satxi qanday nomlanadi | \*Amaliy satx |
|  | Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi | \*Fizik satx |
|  | Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub | \*TCP,UDP |
|  | OSI modelining fizik satxi qanday funktsiyalarni bajaradi | \*Elektr signallarini uzatish va qabul qilish |
|  | OSI modeliningamaliy satxi qanday funktsiyalarni bajaradi | \*Klient dasturlari bilan o’zaro muloqotda bo’lish |
|  | 12 gacha bo’lgan va 12 bilan o’zaro tub bo’lgan sonlar soni nechta? | 6 ta |
|  | Yevklid algoritmi qanday natijani beradi? | \*Sonning eng katta umumiy bo’luvchisini toppish |
|  | Qanday sonlar tub sonlar deb yuritiladi? | \*Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi. |
|  | To‘liq zaxiralash | Tiklashning tezligi yuqori. axira nusxalash jarayonining sekin va ma’lumotni saqlash  uchun ko‘p hajm talab etadi |
|  | O‘sib boruvchi zaxiralash | Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi |
|  | Differnsial zaxiralash | Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma’lumotni saqlash uchun ko‘p hajm talab etadi |
|  | 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 |
|  | Antivirus dasturlarini ko’rsating? | \*Drweb, Nod32, Kaspersky |
|  | Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi | \*wep, wpa, wpa2 |
|  | Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak? | \*ishonchli, qimmatli va to’liq |
|  | Axborotning eng kichik o’lchov birligi nima? | \*bit |
|  | Virtual xususiy tarmoq – bu? | \*VPN |
|  | Xavfli viruslar bu - … | \*kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar |
|  | Mantiqiy bomba – bu … | \*Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari |
|  | Rezident virus... | \*tezkor xotirada saqlanadi |
|  | DIR viruslari nimani zararlaydi? | \*FAT tarkibini zararlaydi |
|  | .... kompyuter tarmoqlari bo’yicha tarqalib, kompyuterning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi | \*«Chuvalchang» va replikatorli virus |
|  | Mutant virus... | \*shifrlash va deshifrlash algoritmlaridan iborat |
|  | Fire Wall ning vazifasi... | \*tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi |
|  | Kompyuter virusi nima? | \*maxsus yozilgan va zararli dastur |
|  | Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating | \*disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali |
|  | Troyan dasturlari bu... | \*virus dasturlar |
|  | Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? | \*5 |
|  | Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud | \*detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar |
|  | Axborotni himoyalash uchun ... usullari qo’llaniladi. | \*kodlashtirish, kriptografiya, stegonografiya |
|  | Stenografiya mahnosi... | \*sirli yozuv |
|  | …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi | \*K.Shennon |
|  | Kriptologiya yo’nalishlari nechta? | \*2 |
|  | Kriptografiyaning asosiy maqsadi... | \*maxfiylik, yaxlitlilikni ta`minlash |
|  | Zararli dasturiy vositalarni aniqlash turlari nechta | \*3 |
|  | Signaiurana asoslangan | \*....bu fayldan topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh  qiymatlari ham signatura sifatida xizmat qilishi mumkin. |
|  | O‘zgarishni aniqlashga asoslangan | ....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. |
|  | 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. |
|  | Antiairuslar qanday usulda viruslarni aniqlaydi | Anomaliyaga asoslangan |
|  | Viruslar - | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Rootkitlar- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Backdoorlar - | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vositasifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Troyan otlari- | \*bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Ransomware- | bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida ko‘rinsada, yashiringan zararli koddan iborat bo‘ladi |
|  | Resurslardan foydalanish usuliga ko’ra viruslar qanday turlarga bo’linadi | \*Virus parazit, Virus cherv |
|  | Zararlagan obyektlar turiga ko’ra | Virus parazit, Virus cherv |
|  | Faollashish prinspiga ko’ra | Virus parazit, Virus cherv |
|  | Dastur kodini tashkil qilish yondashuviga ko‘ra | Virus parazit, Virus cherv |
|  | Shifrlanmagan viruslar | \*o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | Shifrlangan viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | Polimorf viruslar | o‘zini oddiy dasturlar kabi ko‘rsatadi va bunda dastur kodida hech qanday qo‘shimcha ishlashlar mavjud bo‘lmaydi. |
|  | 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. |
|  | 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. |
|  | 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. |
|  | 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. |
|  | Birinchi kompyuter virusi nima deb nomlangan | Cherv |
|  | P= 31, q=29 eyler funksiyasida f(p,q) ni hisoblang | \*840 |
|  | 256mod25=? | 5 |
|  | bu yaxlit «butun»ni tashkil etuvchi bog‘liq yoki o‘zaro bog‘langan tashkil etuvchilar guruhi nima deyiladi. | \*Tizim |
|  | Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori satxli hujjat yoki hujjatlar to‘plami nima duyidadi | Standart |
|  | RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday? | 65535; |
|  | DES algoritmi akslantirishlari raundlari soni qancha? | \*16; |
|  | DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha? | CHap qism blok 32 bit, o‘ng qism blok 48 bit; |
|  | Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? | SHifrlash va deshifrlash jarayonlarida kalitlardan foydalanish qoidalariga ko‘ra farqlanadi |
|  | 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta? | 19 ta |
|  | 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta? | \*4 ta |
|  | Qaysi formula qoldiqli bo’lish qonunini ifodalaydi |  |
|  | Eyler funsiyasida 𝜙(1) qiymati nimaga teng? | \*0 |
|  | Eyler funksiyasida 60 sonining qiymatini toping. | 59 |
|  | Eyler funksiyasi yordamida 1811 sonining qiymatini toping. | \*1810 |
|  | 97 tub sonmi? | \*Tub |
|  | Quyidagi modulli ifodani qiymatini toping  (148 + 14432) mod 256. | \*244 |
|  | Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220 | 21 |
|  | Quyidagi ifodani qiymatini toping.  -17mod11 | 6 |
|  | 2 soniga 10 modul bo’yicha teskari sonni toping. | 3 |

1. I:
2. S: Xavfsizlikning asosiy yo’nalishlarini sanab o’ting.
3. +: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik
4. -: Axborot va Iqtisodiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xafvsizligi, Dasturiy ta`minot xavfsizligi
5. -: Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xafvsizligi, Ekologik xavfsizlik
6. -: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Dasturiy ta`minot xavfsizligi, Ekologik xavfsizlik
7. I:
8. S: Axborot xavfsizligining asosiy maqsadlaridan biri- bu…
9. +: Axborotlarni o’g’irlanishini, yo’qolishini, soxtalashtirilishini oldini olish
10. -:Ob`yektga bevosita ta`sir qilish
11. -: Axborotlarni shifrlash, saqlash, yetkazib berish
12. -: Tarmoqdagi foydalanuvchilarni xavfsizligini ta`minlab berish
13. I:
14. S: Konfidentsiallikga to’g’ri ta`rif keltiring.
15. +: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
16. -:axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati;
17. -:axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati;
18. -:axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati;
19. I:
20. S: Yaxlitlikni buzilishi bu - …
21. +: Soxtalashtirish va o’zgartirish
22. -: Ishonchsizlik va soxtalashtirish
23. -: Soxtalashtirish
24. -: Butunmaslik va yaxlitlanmaganlik
25. I:
26. S:... axborotni himoyalash tizimi deyiladi.
27. +: 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
28. -: 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
29. -: 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
30. -: 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
31. I:
32. S: Kompyuter virusi nima?
33. +: maxsus yozilgan va zararli dastur
34. -:.exe fayl
35. -: boshqariluvchi dastur
36. -: Kengaytmaga ega bo’lgan fayl
37. I:
38. S: Kriptografiyaning asosiy maqsadi...
39. +: maxfiylik, yaxlitlilikni ta`minlash
40. -:ishonchlilik, butunlilikni ta`minlash
41. -:autentifikatsiya, identifikatsiya
42. -:ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya
43. I:
44. S: SMTP - Simple Mail Transfer protokol nima?
45. +: elektron pochta protokoli
46. -:transport protokoli
47. -:internet protokoli
48. -:Internetda ommaviy tus olgan dastur
49. I:
50. S: SKIP protokoli...
51. +: Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi
52. -:Protokollar boshqaruvi
53. -:E-mail protokoli
54. -:Lokal tarmoq protokollari uchun kriptokalitlarning oddiy boshqaruvi
55. I:
56. S: Kompyuter tarmog’ining asosiy komponentlariga nisbatan xavf-xatarlar…
57. +: uzilish, tutib qolish, o’zgartirish, soxtalashtirish
58. -:o’zgartirish, soxtalashtirish
59. -:tutib qolish, o’zgarish, uzilish
60. -:soxtalashtirish, uzilish, o’zgartirish
61. I:
62. S: ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.
63. +: konfidentsiallik
64. -:identifikatsiya
65. -:autentifikatsiya
66. -: maxfiylik
67. I:
68. S: Foydalanish huquqini cheklovchi matritsa modeli bu...
69. +: Bella La-Padulla modeli
70. -:Dening modeli
71. -:Landver modeli
72. -:Huquqlarni cheklovchi model
73. I:
74. S: Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o’rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi?
75. +: TCP/IP, X.25 protokollar
76. -:X.25 protokollar
77. -:TCP/IP
78. -:SMTP
79. I:
80. S: Autentifikatsiya nima?
81. +: Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi
82. -: Tizim meyoriy va g’ayritabiiy hollarda rejalashtirilgandek o’zini tutishligi holati
83. -: Istalgan vaqtda dastur majmuasining mumkinligini kafolati
84. -:Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi
85. I:
86. S:Identifikatsiya bu- …
87. +: Foydalanuvchini uning identifikatori (nomi) bo’yicha aniqlash jarayoni
88. -:Ishonchliligini tarqalishi mumkin emasligi kafolati
89. -:Axborot boshlang’ich ko’rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o’zgarishlar
90. -:Axborotni butunligini saqlab qolgan holda uni elementlarini o’zgartirishga yo’l qo’ymaslik
91. I:
92. S:O’rin almashtirish shifri bu - …
93. +: Murakkab bo’lmagan kriptografik akslantirish
94. -:Kalit asosida generatsiya qilish
95. -:Ketma-ket ochiq matnni ustiga qo’yish
96. -:Belgilangan biror uzunliklarga bo’lib chiqib shifrlash
97. I:
98. S:Simmetrik kalitli shifrlash tizimi necha turga bo’linadi.
99. +: 2 turga
100. -:3 turga
101. -:4 turga
102. -: 5 turga
103. I:
104. S: Kalitlar boshqaruvi 3 ta elementga ega bo’lgan axborot almashinish jarayonidir bular …
105. +: hosil qilish, yig’ish, taqsimlash
106. -:ishonchliligi, maxfiyligi, aniqligi
107. -:xavfsizlik, tez ishlashi, to’g’ri taqsimlanishi
108. -:abonentlar soni, xavfsizligi, maxfiyligi
109. I:
110. S: Kriptologiya -
111. +: axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
112. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
113. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
114. -:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
115. I:
116. S: Kriptografiyada alifbo –
117. +: axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
118. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
119. -:xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
120. -:kalit axborotni shifrlovchi kalitlar
121. I:
122. S: Simmetrik kriptotizimlarda ... jumlani davom ettiring
123. +: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi
124. -:bir-biriga matematik usullar bilan bog’langan ochiq va yopiq kalitlardan foydalaniladi
125. -:axborot ochiq kalit yordamida shifrlanadi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi
126. -:kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi
127. I:
128. S: Kriptobardoshlilik deb …
129. +: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
130. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
131. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
132. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
133. I:
134. S: Elektron raqamli imzo deb –
135. +: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimcha
136. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
137. -:axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
138. -:kalit axborotni shifrlovchi kalitlar
139. I:
140. S: Kriptografiya –
141. +: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
142. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
143. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
144. -:kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
145. I:
146. S: Kriptografiyada matn –
147. +: alifbo elementlarining tartiblangan to’plami
148. -:matnni shifrlash va shifrini ochish uchun kerakli axborot
149. -:axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam
150. -:kalit axborotni shifrlovchi kalitlar
151. I:
152. S: Kriptoanaliz –
153. +: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
154. -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi
155. -:axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi
156. -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi
157. I:
158. S: Shifrlash –
159. +: akslantirish jarayoni ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi
160. -:kalit asosida shifrmatn ochiq matnga akslantiriladi
161. -:shifrlashga teskari jarayon
162. -:Almashtirish jarayoni bo’lib: ochiq matn deb nomlanadigan matn o’girilgan holatga almashtiriladi
163. I:
164. S: Faol hujum turi deb…
165. +: Maxfiy uzatish jarayonini uzib qo’yish, modifikatsiyalash, qalbaki shifr ma`lumotlar tayyorlash harakatlaridan iborat jarayon
166. -:Maxfiy ma`lumotni aloqa tarmog’ida uzatilayotganda eshitish, tahrir qilish, yozib olish harakatlaridan iborat uzatilalayotgan ma`lumotni qabul qiluvchiga o’zgartirishsiz yetkazish jarayoni
167. -:Ma`lumotga o’zgartirish kiritmay uni kuzatish jarayoni
168. -:Sust hujumdan farq qilmaydigan jarayon
169. I:
170. S: Blokli shifrlash-
171. +: shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish
172. -:murakkab bo’lmagan kriptografik akslantirish
173. -:axborot simvollarini boshqa alfavit simvollari bilan almashtirish
174. -:ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi
175. I:
176. S: Simmetrik kriptotizmning uzluksiz tizimida …
177. +: ochiq matnning har bir harfi va simvoli alohida shifrlanadi
178. -:belgilangan biror uzunliklarga teng bo’linib chiqib shifrlanadi
179. -:murakkab bo’lmagan kriptografik akslantirish orqali shifrlanadi
180. -:ketma-ket ochiq matnlarni o’rniga qo’yish orqali shifrlanadi
181. I:
182. S: Kriptotizimga qo’yiladigan umumiy talablardan biri
183. +: shifr matn uzunligi ochiq matn uzunligiga teng bo’lishi kerak
184. -:shifrlash algoritmining tarkibiy elementlarini o’zgartirish imkoniyati bo’lishi lozim
185. -:ketma-ket qo’llaniladigan kalitlar o’rtasida oddiy va oson bog’liqlik bo’lishi kerak
186. -:maxfiylik o’ta yuqori darajada bo’lmoqligi lozim
187. I:
188. S: Berilgan ta`riflardan qaysi biri asimmetrik tizimlarga xos?
189. +: Asimmetrik kriptotizimlarda k1≠k2 bo’lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi
190. -:Asimmetrik tizimlarda k1=k2 bo’ladi, yahni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi
191. -:Asimmetrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma`lum bo’ladi, ochiq kalitni esa faqat qabul qiluvchi biladi
192. -:Asimmetrik kriptotizimlarda k1≠k2 bo’lib, kalitlar hammaga oshkor etiladi
193. I:
194. S: Yetarlicha kriptoturg’unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang
195. +: Vijener matritsasi, Sezar usuli
196. -:monoalfavitli almashtirish
197. -:polialfavitli almashtirish
198. -:o’rin almashtirish
199. I:
200. S: Akslantirish tushunchasi deb nimaga aytiladi?
201. +: 1-to’plamli elementlariga 2-to’plam elementalriga mos bo’lishiga
202. -:1-to’plamli elementlariga 2-to’plam elementalrini qarama-qarshiligiga
203. -:har bir elementni o’ziga ko’payimasiga
204. -:agar birinchi va ikinchi to’plam bir qiymatga ega bulmasa
205. I:
206. S: Simmetrik guruh deb nimaga aytiladi?
207. +: O’rin almashtirish va joylashtirish
208. -:O’rin almashtirish va solishtirish
209. -:Joylashtirish va solishtirish
210. -:O’rin almashtirish va transportizatsiyalash
211. I:
212. S: Qo’yish, o’rin almashtirish, gammalash kriptografiyaning qaysi turiga bog’liq?
213. +: simmetrik kriptosistemalar
214. -:assimetrik kriptosistemalar
215. -:ochiq kalitli kriptosistemalar
216. -:autentifikatsiyalash
217. I:
218. S: Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?
219. +: SMTP, POP yoki IMAP
220. -:SKIP, ATM, FDDI
221. -:X.25 va IMAR
222. -:SMTP, TCP/IP
223. I:
224. S: Axborot resursi – bu?
225. +: axborot tizimi tarkibidagi elektron shakldagi axborot, ma`lumotlar banki, ma`lumotlar bazasi
226. -:cheklanmagan doiradagi shaxslar uchun mo’ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar
227. -:identifikatsiya qilish imkonini beruvchi rekvizitlari qo’yilgan holda moddiy jismda qayd etilgan axborot
228. -:manbalari va taqdim etilish shaklidan qathi nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to’g’risidagi ma`lumotlar
229. I:
230. 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?
231. +: login parol
232. -:identifikatsiya
233. -:maxfiy maydon
234. -: token
235. I:
236. S: Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so’z) – bu?
237. +: parol
238. -:login
239. -:identifikatsiya
240. -:maxfiy maydon foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
241. I:
242. S: Identifikatsiya jarayoni qanday jarayon?
243. +: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
244. -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
245. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
246. -:foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
247. I:
248. S: Autentifikatsiya jarayoni qanday jarayon?
249. +: obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
250. -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
251. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
252. -:foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
253. I:
254. S: Ro’yxatdan o’tish bu?
255. +: foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma`lumotlarni ishlatishga huquq berish jarayoni
256. -:axborot tizimlari ob`yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
257. -:ob`yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash
258. -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
259. I:
260. S: Axborot qanday sifatlarga ega bo’lishi kerak?
261. +: ishonchli, qimmatli va to’liq
262. -:uzluksiz va uzlukli
263. -:ishonchli, qimmatli va uzlukli
264. -:ishonchli, qimmatli va uzluksiz
265. I:
266. S: Axborotning eng kichik o’lchov birligi nima?
267. +: bit
268. -:kilobayt
269. -:bayt
270. -:bitta simvol
271. I:
272. S: Elektron hujjatning rekvizitlari nechta qismdan iborat?
273. +: 4
274. -:5
275. -:6
276. -:7
277. I:
278. S: Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?
279. +: fleshka, CD va DVD disklar
280. -:Qattiq disklar va CDROM
281. -:CD va DVD, DVDROM
282. -:Qattiq disklar va DVDROM
283. I:
284. S: Avtorizatsiya jarayoni qanday jarayon?
285. +: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni
286. -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va -berilgan nom bo’yicha solishtirib uni aniqlash jarayoni
287. -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash.
288. -: parollash jarayoni
289. I:
290. S: Kodlash nima?
291. +: Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir
292. -:Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi
293. mumkin bo‘ladi
294. -:Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi
295. mumkin bo‘ladi
296. -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi
297. I:
298. S: Shifrlash nima?
299. +: Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi
300. -:Ma’lumotni osongina qaytarish uchun hammaga ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirishdir
301. -: Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi
302. -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi
303. I:
304. S: Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi
305. +:Kriptoanaliz
306. -:Kartografiya
307. -:Kriptologiya
308. -:Adamar usuli
309. I:
310. S: Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi
311. +: {d, n} – yopiq, {e, n} – ochiq;
312. -:{d, e} – ochiq, {e, n} – yopiq;
313. -:{e, n} – yopiq, {d, n} – ochiq;
314. -:{e, n} – ochiq, {d, n} – yopiq;
315. I:
316. S: Zamonaviy kriptografiya qanday bo’limlardan iborat?
317. -:Electron raqamli imzo; kalitlarni boshqarish
318. -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;
319. +: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish
320. -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; kalitlarni boshqarish
321. I:
322. S: Shifr nima?
323. +: Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm
324. -:Kalitlarni taqsimlash usuli
325. -:Kalitlarni boshqarish usuli
326. -:Kalitlarni generatsiya qilish usuli
327. I:
328. S: Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?
329. +: Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog’langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi
330. -:Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi
331. -:Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin
332. -:Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat deshifrlash mumkin
333. I:
334. S: Oqimli shifrlashning mohiyati nimada?
335. +: Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,
336. -:Qandaydir ma’lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo’natish uchun oqimli shifrlash zarur,
337. -:Oqimli shifrlash algoritmlari ma’lumotlarnbi bitlar yoki belgilar bo’yicha shifrlaydi
338. -:Oqimli shifrlash birinchi navbatda axborotni bloklarga bo’lishning imkoni bo’lmagan hollarda zarur,
339. I:
340. S: Simmetrik algoritmlarni xavfsizligini ta’minlovchi omillarni ko’rsating.
341. +: 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,
342. -:uzatilayotgan xabarni xavfsizligi kalitni maxfiyligiga emas, balki algoritmni maxfiyligiga bog’liq bo’lishi lozim
343. -:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog’liq bo’lishi lozim
344. -:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga emas, balki shifrlashda foydalaniladigan arifmetik amallar soniga bog’liq bo’lishi lozim
345. I:
346. S: Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?
347. +: shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun
348. -:ERI yaratish va tekshirish, kalitlar almashish uchun
349. -:shifrlash, deshifrlash, kalitlar almashish uchun
350. -: Heshlash uchun
351. I:
352. S: Kriptografik elektron raqamli imzolarda qaysi kalitlar ma’lumotni yaxlitligini ta’minlashda ishlatiladi.
353. +: ochiq kalitlar
354. -:yopiq kalitlar
355. -:seans kalitlari
356. -:Barcha tutdagi kalitlar
357. I:
358. S: Kompyuterning tashqi interfeysi deganda nima tushuniladi?
359. +: kompyuter bilan tashqi qurilmani bog’lovchi simlar va ular orqali axborot almashinish qoidalari to’plamlari
360. -:tashqi qurilmani kompyuterga bog’lashda ishlatiladigan ulovchi simlar
361. -:kompyuterning tashqi portlari.
362. -:tashqi qurilma bilan kompyuter o’rtasida axborot almashinish qoidalari to’plami
363. I:
364. S: Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?
365. +: Yulduz
366. -:Xalqa
367. -:To’liqbog’langan
368. -:Umumiy shina
369. I:
370. S: Ethernet kontsentratori qanday vazifani bajaradi
371. +: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo’naltirib beradi
372. -:kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo’naltirib beradi
373. -:kompyuterdan kelayotgan axborotni xalqa bo’ylab joylashgan keyingi kompyuterga
374. -:tarmoqning ikki segmentini bir biriga ulaydi
375. I:
376. S: OSI modelida nechta satx mavjud
377. +: 7
378. -:4
379. -:5
380. -:3
381. I:
382. S: OSI modelining to’rtinchi satxi qanday nomlanadi
383. +: Transport satxi
384. -:Amaliy satx
385. -:Seanslar satxi
386. -:Taqdimlash satxi
387. I:
388. S: OSI modelining beshinchi satxi qanday nomlanadi
389. +: Seanslar satxi
390. -:Tarmoq satxi
391. -:Fizik satx
392. -:Amaliy satx
393. I:
394. S: OSI modelining birinchi satxi qanday nomlanadi
395. +: Fizik satx
396. -:Seanslar satxi
397. -:Transport satxi
398. -:Taqdimlash satxi
399. I:
400. S: OSI modelining ikkinchi satxi qanday nomlanadi
401. +: Kanal satxi
402. -:Amaliy satxi
403. -:Fizik satx
404. -:Seanslar satxi
405. I:
406. S: OSI modelining uchinchi satxi qanday nomlanadi
407. +: Tarmoq satxi
408. -:Amaliy satx
409. -:Kanal satxi
410. -:Taqdimlash satxi
411. I:
412. S: OSI modelining oltinchi satxi qanday nomlanadi
413. +: Taqdimlash satxi
414. -:Amaliy satx
415. -:Seanslar satxi
416. -:Kanal satxi
417. I:
418. S: OSI modelining yettinchi satxi qanday nomlanadi
419. +: Amaliy satx
420. -:Seanslar satxi
421. -:Transport satxi
422. -:Taqdimlash satxi
423. I:
424. S: OSI modelining qaysi satxlari tarmoqqa bog’liq satxlar hisoblanadi
425. +: fizik, kanal va tarmoq satxlari
426. -:seans va amaliy satxlar
427. -:amaliy va taqdimlash satxlari
428. -:transport va seans satxlari
429. I:
430. S: OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi
431. +: Marshrutizator
432. -:Ko’prik
433. -:Tarmoq adapter
434. -:Kontsentrator
435. I:
436. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
437. +: Fizik satx
438. -:Kanal satxi
439. -:Tarmoq satxi
440. -:Transport satxi
441. I:
442. S: Ma’lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi
443. +: Tarmoq satxi
444. -:Kanal satxi
445. -:Amaliy satx
446. -:Transport satxi
447. I:
448. S: Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub
449. +: IP, IPX
450. -:NFS, FTP
451. -:Ethernet, FDDI
452. -:TCP,UDP
453. I:
454. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
455. +: TCP,UDP
456. -:NFS, FTP
457. -:IP, IPX
458. -:Ethernet, FDDI
459. I:
460. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
461. +: Elektr signallarini uzatish va qabul qilish
462. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojaat qilishni boshqarish
463. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
464. -:Klient dasturlari bilan o’zaro muloqotda bo’lish
465. I:
466. S: Identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayoni bu...
467. +: Avtorizatsiya
468. -:Shifrlash
469. -:Identifikatsiya
470. -:Autentifikatsiya
471. I:
472. S: Autentifikatsiya faktorlari nechta
473. +: 3
474. -:4
475. -:5
476. -: 6
477. I:
478. S: Ko‘z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar?
479. +: Biometrik autentifikatsiya
480. -:Biron nimaga egalik asosida
481. -:Biron nimani bilish asosida
482. -:Parolga asoslangan
483. I:
484. 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?
485. +: Fizik satx
486. -:Tarmoq satxi
487. -:Amaliy satx
488. -:Tadbiqiy sath
489. I:
490. S: Fizik xavfsizlikda Yong‘inga qarshi tizimlar necha turga bo‘linadi
491. +: 2
492. -:4
493. -:3
494. -:5
495. I:
496. S: Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?
497. +: Subyekt
498. -:Obyekt
499. -:Tizim
500. -:Jarayon
501. I:
502. S: MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi
503. +: xavfsizlik siyosati ma’muri
504. -:Foydalaguvchining o‘zi
505. -:Dastur tomonidan
506. -:Boshqarish amaalga oshirilmaydi
507. I:
508. S: Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda uchun qanday amalga ruxsat beriladi
509. +: O‘qish
510. -:Yozish
511. -:O‘zgartirish
512. -:Yashirish
513. I:
514. S: Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo‘lsa, u holda qanday amalga ruxsat beriladi.
515. +: Yozish
516. -:O‘qish
517. -:O‘zgartirish
518. -:Yashirish
519. I:
520. S: Rol tushunchasiga ta’rif bering.
521. +: Muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin
522. -:Foydalanishni boshqarish
523. -:Muayyan faoliyat turi bilan bog‘liq imkoniyatlar to‘plami sifatida belgilanishi mumkin
524. -:Vakolitlarni taqsimlash
525. I:
526. 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.
527. +: ABAC
528. -:MAC
529. -:DAC
530. -:RBAC
531. I:
532. S: Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan avfzalliklari qaysi javobda to‘g‘ri ko‘rsatilgan?
533. +: barchasi
534. -:bimetrik alomatlarning ishga layoqatli shaxsdan ajratib bo‘lmasligi
535. -:biometrik alomatlarni soxtalashtirishning qiyinligi
536. -:biometrik alomatlarni noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasi yuqoriligi
537. I:
538. S: OSI modeli 7 satxi bu
539. +: Ilova
540. -:Seans
541. -:Fizik
542. -:Kanal
543. I:
544. S: OSI modeli 1 satxi bu
545. +: Fizik
546. -:Ilova
547. -:Seans
548. -:Kanal
549. I:
550. S: OSI modeli 2 satxi bu
551. +:Kanal
552. -: Fizik
553. -:Ilova
554. -:Seans
555. I:
556. S: TCP/IP modelida nechta satx mavjud
557. +: 4
558. -:3
559. -:2
560. -:8
561. I:
562. S: Qanday tarmoq qisqa masofalarda qurilmalar o‘rtasid a ma’lumot almashinish imkoniyatini taqdim etadi?
563. +: Shaxsiy tarmoq
564. -:Lokal
565. -:Mintaqaviy
566. -:CAMPUS
567. I:
568. S: Tarmoq kartasi bu...
569. +: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
570. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.
571. -:ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
572. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
573. I:
574. S: Server xotirasidagi joyni bepul yoki pulli ijagara berish xizmati qanday ataladi?
575. +: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
576. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
577. -:Signalni tiklash yoki qaytarish uchun foydalaniladi.
578. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
579. I:
580. S: Hab bu...
581. +: ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
582. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
583. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.
584. -:qabul qilingan signalni barchachiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
585. I:
586. S: Tarmoq repiteri bu...
587. +: Signalni tiklash yoki qaytarish uchun foydalaniladi.
588. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.
589. -:ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
590. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.
591. I:
592. S: Qanday tizim host nomlari va internet nomlarini IP manzillarga o‘zgartirish yoki teskarisini amalga oshiradi.
593. +: DNS tizimlari
594. -:TCP/IP
595. -:Ethernet
596. -:Token ring
597. I:
598. S: ….. protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.
599. +: TCP
600. -:IP
601. -:HTTP
602. -:FTP
603. I:
604. S: …. protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi.
605. +: UDP
606. -:HTTP
607. -:TCP
608. -:FTP
609. I:
610. S: Qaysi protokol ma’lumotni yuborishdan oldin aloqa o‘rnatish uchun zarur bo‘lgan manzil ma’lumotlari bilan ta’minlaydi.
611. +: IP
612. -:TCP
613. -:HTTP
614. -:FTP
615. I:
616. S: Tarmoq taxdidlari necha turga bo‘linadi
617. +: 4
618. -:2
619. -:3
620. -:5
621. I:
622. S: Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;
623. +: Razvedka hujumlari
624. -:Kirish hujumlari
625. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
626. -:Zararli hujumlar
627. I:
628. S: Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi
629. +: Kirish hujumlari
630. -:Razvedka hujumlari
631. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
632. -:Zararli hujumlar
633. I:
634. S: Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;
635. +: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
636. -:Razvedka hujumlari
637. -:Kirish hujumlari
638. -:Zararli hujumlar
639. I:
640. S: Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;
641. +: Zararli hujumlar
642. -:Razvedka hujumlari
643. -:Kirish hujumlari
644. -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari
645. I:
646. S: RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart?
647. +: e soni Eyler funksiyasi -bilan o‘zaro tub
648. -:e ning qiymati [1,n] kesmaga tegishli ixtiyoriy son
649. -:e soni ixtiyoriy tub son
650. -:e soni ixtiyoriy butun musbat son
651. I:
652. S: RSA elektron raqamli imzo algoritmidagi yopiq kalit d qanday hisoblanadi? Bu yerda p va q tub sonlar,n=pq,- Eyler funksiyasi,e-ochiq kalit
653. +:
654. -:
655. -:
656. -:
657. I:
658. S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?
659. +: Imzo qo‘yish va imzoni tekshirishdan
660. -:Faqat imzo qo‘yishdan
661. -:Faqat imzoni tekshirishdan
662. -:Barcha javoblar to‘g‘ri
663. I:
664. S: Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi?
665. +: Imzo muallifining ochiq kaliti yordamida
666. -:Ma’lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida
667. -:Ma’lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida
668. -:Imzo muallifining maxfiy kaliti yordamida
669. I:
670. S: Tarmoq modeli-bu...
671. +: Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqqiyatli o‘rnatilishini asosidir
672. -:Global tarmoq qurish usullari
673. -:Lokal tarmoq qurish usullari
674. -:To‘g‘ri javob yo‘q.
675. I:
676. S: OSI modeli nechta satxga ajraladi?
677. +: 7
678. -:2
679. -:4
680. -:3
681. I:
682. S: TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi
683. +: Kanal, Fizik
684. -:Tarmoq
685. -:Tramsport
686. -:Ilova, taqdimot, seans.
687. I:
688. S: TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi
689. +: Tarmoq
690. -:Kanal, Fizik
691. -:Tramsport
692. -:Ilova, taqdimot, seans.
693. I:
694. S: TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi
695. +: Tramsport
696. -:Kanal, Fizik
697. -:Tarmoq
698. -:Ilova, taqdimot, seans.
699. I:
700. S: TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos keladi
701. +: Ilova, taqdimot, seans
702. -:Kanal, Fizik
703. -:Tarmoq
704. -:Tramsport
705. I:
706. S: Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.
707. +: Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
708. -:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
709. -:Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi
710. -:Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi
711. I:
712. S: Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang.
713. +: Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi.
714. -:Kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi.
715. -:Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi
716. -:Qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi.
717. I:
718. S: Repetir nima?
719. +: Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
720. -:Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
721. -: Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi
722. -: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
723. I:
724. S: Hub nima?
725. +: Tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi
726. -:Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi, Odatda signalni tiklash yoki qaytarish uchun foydalaniladi
727. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
728. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
729. I:
730. S: Router nima?
731. +: Qabul qilingan ma’lumotlarni tarmoq satxiga tegishli manzillarga ko‘ra (IP manzil) uzatadi.
732. -: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
733. -:Ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi.
734. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi
735. I:
736. S: Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqasadda amalga oshiriladigan tarmoq hujumi qaysi
737. +: Razvedka hujumlari
738. -:Kirish hujumlari
739. -:DOS hujumi
740. -:Zararli hujumlar
741. I:
742. S: Razvedka hujumiga berilgan ta’rifni aniqlang
743. +: Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi;
744. -:hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi hujumchi -:mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi;
745. -:zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi;
746. I:
747. S: OSI modelining birinchi satxi qanday nomlanadi
748. +: Fizik satx
749. -:Seanslar satxi
750. -:Transport satxi
751. -:Taqdimlash satxi
752. I:
753. S: OSI modelining ikkinchi satxi qanday nomlanadi
754. +: Kanal satxi
755. -:Amaliy satxi
756. -:Fizik satx
757. -:Seanslar satxi
758. I:
759. S: OSI modelining uchinchi satxi qanday nomlanadi
760. +: Tarmoq satxi
761. -:Amaliy satx
762. -:Kanal satxi
763. -:Taqdimlash satxi
764. I:
765. S: OSI modelining oltinchi satxi qanday nomlanadi
766. +: Taqdimlash satxi
767. -:Amaliy satx
768. -:Seanslar satxi
769. -:Kanal satxi
770. I:
771. S: OSI modelining ettinchi satxi qanday nomlanadi
772. +: Amaliy satx
773. -:Seanslar satxi
774. -:Transport satxi
775. -:Taqdimlash satxi
776. I:
777. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
778. +: Fizik satx
779. -:Kanal satxi
780. -:Tarmoq satxi
781. -:Transport satxi
782. I:
783. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
784. +: TCP,UDP
785. -:NFS, FTP
786. -:IP, IPX
787. -:Ethernet, FDDI
788. I:
789. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
790. +: Elektr signallarini uzatish va qabul qilish
791. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
792. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
793. -:Klient dasturlari bilan o’zaro muloqotda bo’lish
794. I:
795. S: OSI modelining amaliy satxi qanday funksiyalarni bajaradi
796. +: Klient dasturlari bilan o’zaro muloqotda bo’lish
797. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
798. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
799. -:Elektr signallariniuzatish va qabul qilish
800. I:
801. S: Yevklid algoritmi qanday natijani beradi?
802. +: Sonning eng katta umumiy bo’luvchisini toppish
803. -:Sonning turli bo’luvchilarini toppish
804. -:Sonning eng kichik umumiy karralisini toppish
805. -:Sonning eng katta umumiy bo’linuvchisini topish
806. I:
807. S: Qanday sonlar tub sonlar deb yuritiladi?
808. +: Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi.
809. -:O’zidan boshqa bo’luvchilari mavjud bo’lgan sonlar tub sonlar deyiladi.
810. -:Agar sonning 1 dan boshqa bo’luvchilari bo’lsa.
811. -:Faqatgina 1 ga o’ziga bo’linmaydigan sonlar tub sonlar deyiladi.
812. I:
813. S: OSI modelining birinchi satxi qanday nomlanadi
814. +: Fizik satx
815. -:Seanslar satxi
816. -:Transport satxi
817. -:Taqdimlash satxi
818. I:
819. S: OSI modelining ikkinchi satxi qanday nomlanadi
820. +: Kanal satxi
821. -:Amaliy satxi
822. -:Fizik satx
823. -:Seanslar satxi
824. I:
825. S: OSI modelining uchinchi satxi qanday nomlanadi
826. +: Tarmoq satxi
827. -:Amaliy satx
828. -:Kanal satxi
829. -:Taqdimlash satxi
830. I:
831. S: OSI modelining oltinchi satxi qanday nomlanadi
832. +: Taqdimlash satxi
833. -:Amaliy satx
834. -:Seanslar satxi
835. -:Kanal satxi
836. I:
837. S: OSI modelining ettinchi satxi qanday nomlanadi
838. +: Amaliy satx
839. -:Seanslar satxi
840. -:Transport satxi
841. -:Taqdimlash satxi
842. I:
843. S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi
844. +: Fizik satx
845. -:Kanal satxi
846. -:Tarmoq satxi
847. -:Transport satxi
848. I:
849. S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub
850. +: TCP,UDP
851. -:NFS, FTP
852. -:IP, IPX
853. -:Ethernet, FDDI
854. I:
855. S: OSI modelining fizik satxi qanday funktsiyalarni bajaradi
856. +: Elektr signallarini uzatish va qabul qilish
857. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
858. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
859. -:Klient dasturlari bilan o’zaro muloqotda bo’lish
860. I:
861. S: OSI modeliningamaliy satxi qanday funktsiyalarni bajaradi
862. +: Klient dasturlari bilan o’zaro muloqotda bo’lish
863. -:Aloqa kanalini va ma’lumotlarni uzatish muxitiga murojat qilishni boshqarish
864. -:Bog’lanish seansini yaratish, kuzatish, oxirigacha ta’minlash
865. -:Elektr signallariniuzatish va qabul qilish
866. I:
867. S: Yevklid algoritmi qanday natijani beradi?
868. +: Sonning eng katta umumiy bo’luvchisini toppish
869. -:Sonning turli bo’luvchilarini toppish
870. -:Sonning eng kichik umumiy karralisini toppish
871. -:Sonning eng katta umumiy bo’linuvchisini topish
872. I:
873. S: Qanday sonlar tub sonlar deb yuritiladi?
874. +: Faqatgina 1 ga va o’ziga bo’linadigan sonlar tub sonlar deyiladi.
875. -:O’zidan boshqa bo’luvchilari mavjud bo’lgan sonlar tub sonlar deyiladi.
876. -:Agar sonning 1 dan boshqa bo’luvchilari bo’lsa.
877. -:Faqatgina 1 ga o’ziga bo’linmaydigan sonlar tub sonlar deyiladi.
878. I:
879. S: Antivirus dasturlarini ko’rsating?
880. +: Drweb, Nod32, Kaspersky
881. -:arj, rar, pkzip, pkunzip
882. -:winrar, winzip, winarj
883. -:pak, lha
884. I:
885. S: Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi
886. +: wep, wpa, wpa2
887. -:web, wpa, wpa2
888. -:wpa, wpa2
889. -:wpa, wpa2, wap
890. I:
891. S: Axborot himoyalangan qanday sifatlarga ega bo’lishi kerak?
892. +: ishonchli, qimmatli va to’liq
893. -:uzluksiz va uzlukli
894. -:ishonchli, qimmatli va uzlukli
895. -:ishonchli, qimmatli va uzluksiz
896. I:
897. S: Axborotning eng kichik o’lchov birligi nima?
898. +: bit
899. -:kilobayt
900. -:bayt
901. -:bitta simvol
902. I:
903. S: Virtual xususiy tarmoq – bu?
904. +: VPN
905. -:APN
906. -:ATM
907. -:Ad-hoc
908. I:
909. S: Xavfli viruslar bu - …
910. +: kompyuter ishlashida jiddiy nuqsonlarga sabab bo’luvchi viruslar
911. -:tizimda mavjudligi turli taassurot (ovoz, video) bilan bog’liq viruslar, bo’sh xotirani kamaytirsada, dastur va ma`lumotlarga ziyon yetkazmaydi
912. -:o’z-o’zidan tarqalish mexanizmi amalga oshiriluvchi viruslar
913. -:dastur va ma`lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o’chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar
914. I:
915. S: Mantiqiy bomba – bu …
916. +: Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari
917. -:Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari
918. -:Viruslar kodiga boshqarishni uzatish
919. -:Qidirishning passiv mexanizmlarini amalga oshiruvchi, yahni dasturiy fayllarga tuzoq qo’yuvchi viruslar
920. I:
921. S: Rezident virus...
922. +: tezkor xotirada saqlanadi
923. -:to’liqligicha bajarilayotgan faylda joylashadi
924. -:ixtiyoriy sektorlarda joylashgan bo’ladi
925. -:alohida joyda joylashadi
926. I:
927. S: DIR viruslari nimani zararlaydi?
928. +: FAT tarkibini zararlaydi
929. -:com, exe kabi turli fayllarni zararlaydi
930. -:yuklovchi dasturlarni zararlaydi
931. -:Operatsion tizimdagi sonfig.sys faylni zararlaydi
932. I:
933. S:.... kompyuter tarmoqlari bo’yicha tarqalib, komlg’yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o’zining nusxasini qoldiradi
934. +: «Chuvalchang» va replikatorli virus
935. -:Kvazivirus va troyan virus
936. -:Troyan dasturi
937. -:Mantiqiy bomba
938. I:
939. S: Fire Wall ning vazifasi...
940. +: tarmoqlar orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi
941. -:kompyuterlar tizimi xavfsizligini ta`minlaydi
942. -:Ikkita kompyuter o’rtasida aloqa o’rnatish jarayonida Internet tarmog’i orasida xavfsizlikni ta`minlaydi
943. -:uy tarmog’i orasida aloqa o’rnatish jarayonida tashkilot va Internet tarmog’i orasida xavfsizlikni ta`minlaydi
944. I:
945. S: Kompyuter virusi nima?
946. +: maxsus yozilgan va zararli dastur
947. -:.exe fayl
948. -:boshqariluvchi dastur
949. -:Kengaytmaga ega bo’lgan fayl
950. I:
951. S: Kompyuterning viruslar bilan zararlanish yo’llarini ko’rsating
952. +: disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali
953. -: faqat maxsus tashuvchi qurilma orqali
954. -: faqat kompyuter tarmoqlari orqali
955. -:zararlanish yo’llari juda ko’p
956. I:
957. S: Troyan dasturlari bu...
958. +: virus dasturlar
959. -:antivirus dasturlar
960. -:o’yin dasturlari
961. -:yangilovchi dasturlar
962. I:
963. S: Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi?
964. +: 5
965. -:4
966. -:2
967. -:3
968. I:
969. S: Antiviruslarni, qo’llanish usuliga ko’ra... turlari mavjud
970. +: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar
971. -:detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar
972. -:vaktsinalar, privivkalar, revizorlar, tekshiruvchilar
973. -:privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar
974. I:
975. S: Stenografiya mahnosi...
976. +: sirli yozuv
977. -:sirli xat
978. -:maxfiy axborot
979. -:maxfiy belgi
980. I:
981. S: …sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi
982. +: K.Shennon
983. -:Sezar
984. -:U.Xill
985. -:Fon Neyman
986. I:
987. S: Kriptologiya yo’nalishlari nechta?
988. +: 2
989. -:3
990. -:4
991. -:5
992. I:
993. S: Kriptografiyaning asosiy maqsadi...
994. +: maxfiylik, yaxlitlilikni ta`minlash
995. -:ishonchlilik, butunlilikni ta`minlash
996. -:autentifikatsiya, identifikatsiya
997. -:ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya
998. I:
999. S: DES algoritmi akslantirishlari raundlari soni qancha?
1000. +: 16;
1001. -:14;
1002. -:12;
1003. -:32;
1004. I:
1005. S: DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha?
1006. +: CHap qism blok 32 bit, o‘ng qism blok 32 bit;
1007. -:CHap qism blok 32 bit, o‘ng qism blok 48 bit;
1008. -:CHap qism blok 64 bit, o‘ng qism blok 64 bit;
1009. -:CHap qism blok 16 bit, o‘ng qism blok 16 bit;
1010. I:
1011. S: 19 gacha bo’lgan va 19 bilan o’zaro tub bo’lgan sonlar soni nechta?
1012. +: 18 ta;
1013. -:19 ta
1014. -:11 ta
1015. -:9 ta
1016. I:
1017. S: 10 gacha bo’lgan va 10 bilan o’zaro tub bo’lgan sonlar soni nechta?
1018. +: 3 ta
1019. -:7 ta
1020. -:8 ta;
1021. -:9 ta
1022. I:
1023. S: Qaysi formula qoldiqli bo’lish qonunini ifodalaydi
1024. +: a = bq + r, ,
1025. -:
1026. -:M=r1^k2;
1027. -:M=
1028. I:
1029. S: Eyler funksiyasida p=11 va q=13 sonining qiymatini toping.
1030. +: 16
1031. -:59
1032. -:30
1033. -:21
1034. I:
1035. S: Eyler funksiyasi yordamida 1811 sonining qiymatini toping.
1036. +: 1810
1037. -:2111
1038. -:16
1039. -:524
1040. I:
1041. S: 97 tub sonmi?
1042. +: Tub
1043. -:murakkab
1044. -:Natural
1045. -:To’g’ri javob yo’q
1046. I:
1047. S: Quyidagi modulli ifodani qiymatini toping
1048. (148 + 14432) mod 256.
1049. +: 244
1050. -:200
1051. -:156
1052. -:154
1053. I:
1054. S: Quyidagi sonlarning eng katta umumiy bo’luvchilarini toping. 88 i 220
1055. +: 44
1056. -:21
1057. -:42
1058. -:20
1059. I:
1060. S: Quyidagi ifodani qiymatini toping. -16mod11
1061. +: 6
1062. -:5
1063. -:7
1064. -:11
1065. I:
1066. S: 2 soniga 10 modul bo’yicha teskari sonni toping.
1067. +: Ø
1068. -:3
1069. -:10
1070. -:25
1071. I:
1072. S: 2 soniga 10 modul bo’yicha teskari sonni toping.
1073. +: Ø
1074. -:3
1075. -:10
1076. -:25
1077. I:
1078. S: DES da dastlabki kalit uzunligi necha bitga teng?
1079. +:56 bit
1080. -:128 bit
1081. -:64 bit
1082. -:32 bit
1083. I:
1084. S: DES da bloklar har birining uzunligi necha bitga teng?
1085. +:32 bit
1086. -:56 bit
1087. -:48 bit
1088. -:64 bit
1089. I:
1090. S: DES da raundlar soni nechta?
1091. +:16
1092. -:32
1093. -:8
1094. -:48
1095. I:
1096. S: Shifrlash kaliti noma’lum bo’lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi
1097. +:kriptobardoshlik
1098. -:Shifr matn uzunligi
1099. -:Shifrlash algoritmi
1100. -:Texnika va texnologiyalar
1101. I:
1102. S: Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo’linadi
1103. +:blokli va oqimli
1104. -:DES va oqimli
1105. -:Feystel va Verman
1106. -:SP− tarmoq va IP
1107. I:
1108. S: DES shifrlash algoritmida shifrlanadigan malumotlar bloki necha bit?
1109. +:64
1110. -:32
1111. -:48
1112. -:56
1113. I:
1114. S: XOR amali qanday amal?
1115. +:2 modul bo`yicha qo`shish
1116. -:264 modul bo`yicha qo`shish
1117. -:232 modul bo`yicha qo`shish
1118. -:248 modul bo`yicha qo`shish
1119. I:
1120. S: 4+31 mod 32 ?
1121. +:3
1122. -:4
1123. -:31
1124. -:32
1125. I:
1126. S: 21+20mod32?
1127. +:9
1128. -:12
1129. -:16
1130. -:41
1131. I:
1132. S: 12+22 mod 32 ?
1133. +:2
1134. -:12
1135. -:22
1136. -:32
1137. I:
1138. S: AES algoritmi bloki uzunligi … bitdan kam bo’lmasligi kerak.
1139. +:128
1140. -:512
1141. -:256
1142. -:192
1143. I:
1144. S: Xesh-:funktsiyani natijasi …
1145. +:fiksirlangan uzunlikdagi xabar
1146. -:Kiruvchi xabar uzunligidagi xabar
1147. -:Kiruvchi xabar uzunligidan uzun xabar
1148. -:fiksirlanmagan uzunlikdagi xabar
1149. I:
1150. S: 2+5 mod32 ?
1151. +:7
1152. -:32
1153. -:2
1154. -:5
1155. I:
1156. S: 97 tub sonmi?
1157. +:Tub
1158. -:murakkab
1159. -:Natural
1160. -:To’g’ri javob yo’q
1161. I:
1162. S: Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing.
1163. +:23
1164. -:20
1165. -:21
1166. -:19
1167. I:
1168. S: Quyidagi ifodani qiymatini toping. -17mod11
1169. +:5
1170. -:6
1171. -:7
1172. -:11
1173. I:
1174. S: Diskni shifrlash nima uchun amalga oshiriladi?
1175. +: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
1176. -:Xabarni yashirish uchun amalga oshiriladi
1177. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi
1178. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi
1179. I:
1180. S: Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?
1181. +: 4
1182. -:8
1183. -:7
1184. -:5
1185. I:
1186. S: OSI modelida nechta tarmoq satxi bor
1187. +: 7
1188. -:6
1189. -:5
1190. -:4
1191. I:
1192. S: Diskni shifrlash nima uchun amalga oshiriladi?
1193. +: Ma’lumotni saqlash vositalarida saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi
1194. -:Xabarni yashirish uchun amalga oshiriladi
1195. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot butunligini ta’minlash uchun amalga oshiriladi
1196. -:Ma’lumotni saqlash vositalarida saqlangan ma’lumot foydalanuvchanligini ta’minlash uchun amalga oshiriladi
1197. I:
1198. S: Ma’lumotlarni yo‘q qilish odatda necha hil usulidan foydalaniladi?
1199. +: 4
1200. -:8
1201. -:7
1202. -:5
1203. I:
1204. S: OSI modelida nechta tarmoq satxi bor
1205. +: 7
1206. -:6
1207. -:5
1208. -:4
1209. I:
1210. S: “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonun moddadan iborat
1211. +:16
1212. -:18
1213. -:11
1214. -:14
1215. I:
1216. S: Kompyuter etikasi instituti notijoriy tashkilot tomonidan texnologiyani axloqiy nuqta nazardan targ‘ib qilish bo‘yicha nechta etika qoidalari keltirilgan
1217. +:10
1218. -:18
1219. -:11
1220. -:14
1221. I:
1222. S: Kiberjinoyatchilik bu –. . .
1223. +: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.
1224. -: Kompyuter o‘yinlari
1225. -: Faqat banklardan pul o‘g‘irlanishi
1226. -: autentifikatsiya jarayonini buzish
1227. I:
1228. S: Fishing nima?
1229. +: Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir.
1230. -: Ma’lumotlar bazalarini xatoligi
1231. -: Mualliflik huquqini buzilishi
1232. -: Lug‘at orqali xujum qilish.
1233. I:
1234. S: Bag nima?
1235. +: Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo
1236. -: Mualliflik huquqini buzilishi
1237. -: Dasturlardagi ortiqcha reklamalar
1238. -: Autentifikatsiya jarayonini buzish
1239. I:
1240. S: Nuqson nima?
1241. +: Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi nuqsondir
1242. -: Dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo‘lgan muammo
1243. -: Dasturlardagi ortiqcha reklamalar
1244. -: Autentifikatsiya jarayonini buzish
1245. I:
1246. S: Quyidagilardan qaysi birida xavfsiz dasturlash tillari keltirilgan.
1247. +: C#, Scala, Java
1248. -: C, C#, java
1249. -: C++, Scala, Java
1250. -: Misra-C, Java, c++
1251. I:
1252. S: Quyidagilardan qaysi biri dasturiy maxsulotlarga qo‘yiladigan xavfsizlik talablari hisoblanidi.
1253. +: Vazifaviy, novazifaviy, qolgan talablar
1254. -: Qolgan talablar, anaviy taablar, etika talablari
1255. -: Vazifaviy, novazifaviy, etika talablari.
1256. -: Vazifaviy, etika talablari, foydalanuvchanlik talablari.
1257. I:
1258. S: Dasturiy ta’minotda kirish va chiqishga aloqador bo‘lgan talablar qanday talablar sirasiga kiradi?
1259. +:Vazifaviy
1260. -: Novazifaviy
1261. -: Etika talablari
1262. -: Qolgan talablar
1263. I:
1264. S: Dasturda tizim amalga oshirishi kerak bo‘lgan vazifalar bu..
1265. +:Vazifaviy
1266. -: Novazifaviy
1267. -: Etika talablari
1268. -: Qolgan talablar
1269. I:
1270. S: Risklarni boshqarishda risklarni aniqlash jarayoni bu-..
1271. +: Tashkilot xavfsizligiga ta’sir qiluvchi tashqi va ichki risklarning manbasi, sababi, oqibati va haklarni aniqlash.
1272. -: Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta’siri va ehtimolini o‘lchashni ta’minlaydi.
1273. -: Risklarni davolash bu – aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni.
1274. -: Risk monitoringi yangi risklarni paydo bo‘lish imkoniyatini aniqlash.
1275. I:
1276. S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.
1277. +:"Sovuq saxiralash"
1278. -:"Issiq zaxiralash"
1279. -:"Iliq saxiralash"
1280. -:"To'liq zaxiralash"
1281. I:
1282. S: Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishi bilan bog'liq bo'lsa bu nima deb yuritiladi?
1283. +:Jinoyat sifatida baholanadi
1284. -:Rag’bat hisoblanadi
1285. -:Buzgunchilik hisoblanadi
1286. -:Guruhlar kurashi hisoblanadi
1287. I:
1288. S: Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun qanday kalit ishlatiladi?
1289. +:Ikkita kalit
1290. -:Bitta kalit
1291. -:Elektron raqamli imzo
1292. -:Foydalanuvchi identifikatori
1293. I:
1294. S:Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?
1295. +:Axborot xavfsizligi buzulgan taqdirda ko’rilishi mumkin bo’lgan zarar miqdori bilan
1296. -:Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhumligi bilan
1297. -:Axborotni noqonuniy foydalanishlardan o’zgartirishlardan va yo’q qilishlardan himoyalanganligi bilan
1298. -:Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bilan}
1299. I:
1300. S:Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?
1301. +:Strukturalarni ruxsatsiz modifikatsiyalash
1302. -:Tabiy ofat va avariya
1303. -:Texnik vositalarning buzilishi va ishlamasligi
1304. -:Foydalanuvchilar va xizmat ko‘rsatuvchi hodimlarning hatoliklari}
1305. I:
1306. S:Axborot xavfsizligiga bo‘ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?
1307. +:Texnik vositalarning buzilishi va ishlamasligi
1308. -:Axborotdan ruhsatsiz foydalanish
1309. -:Zararkunanda dasturlar
1310. -:An’anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili}
1311. I:
1312. S:Axborot xavfsizligini ta'minlovchi choralarni ko’rsating?
1313. +:1-huquqiy, 2-tashkiliy-ma'muriy, 3-injener-texnik
1314. -:1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy
1315. -:1-dasturiy, 2-tashkiliy-ma'muriy, 3-huquqiy
1316. -:1-aparat, 2-texnikaviy, 3-huquqiy}
1317. I:
1318. S:Axborot xavfsizligining huquqiy ta'minoti qaysi me’yorlarni o’z ichiga oladi
1319. +:Xalqaro va milliy huquqiy me’yorlarni
1320. -:Tashkiliy va xalqaro me’yorlarni
1321. -:Ananaviy va korporativ me’yorlarni
1322. -:Davlat va nodavlat tashkilotlarime’yorlarni}
1323. I:
1324. S:Axborotni uzatish va saqlash jarayonida o‘z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?
1325. +: Ma’lumotlar butunligi
1326. -:Axborotning konfedensialligi
1327. -:Foydalanuvchanligi
1328. -:Ixchamligi}
1329. I:
1330. S:Axborotning buzilishi yoki yo‘qotilishi xavfiga olib keluvchi himoyalanuvchi ob’ektga qarshi qilingan xarakatlar qanday nomlanadi?
1331. +:Tahdid
1332. -:Zaiflik
1333. -:Hujum
1334. -:Butunlik}
1335. I:
1336. S:Biometrik autentifikatsiyalashning avfzalliklari-bu:
1337. +:Biometrik alomatlarning noyobligi
1338. -:Bir marta ishlatilishi
1339. -:Biometrik alomatlarni o’zgartirish imkoniyati
1340. -:Autentifikatsiyalash jarayonining soddaligi
1341. I:
1342. S: Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari-bu:
1343. +:Foydalanuvchanligi
1344. -:Ma’lumotlar butunligi
1345. -:Axborotning konfedensialligi
1346. -:Ixchamligi
1347. I:
1348. S:Global simsiz tarmoqning ta`sir doirasi qanday?
1349. +:Butun dunyo bo’yicha
1350. -:Binolar va korpuslar
1351. -:O’rtacha kattalikdagishahar
1352. -:Foydalanuvchi yaqinidagi tarmoq
1353. I:
1354. S: Foydalanuvchini identifikatsiyalashda qanday ma’lumotdan foydalaniladi?
1355. +:Identifikatori
1356. -:Telefon raqami
1357. -:Parol
1358. -:Avtorizatsiyasi
1359. I:
1360. S: Foydalanuvchining tarmoqdagi harakatlarini va resurslardan foydalanishga urinishini qayd etish-bu:
1361. +:Ma`murlash
1362. -:Autentifikatsiya
1363. -:Identifikatsiya
1364. -:Sertifikatsiyalash
1365. I:
1366. 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?
1367. +:Injener-texnik
1368. -:Molyaviy
1369. -:Tashkiliy-ma’muriy
1370. -:Huquqiy
1371. I:
1372. S: Ma`lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi-bu:
1373. +:Autentifikatsiya
1374. -:Identifikatsiya
1375. -:Ma`murlash (accaunting)
1376. -:Avtorizatsiya
1377. I:
1378. S: O‘zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi–bu:
1379. +:Tarmoq viruslari
1380. -:Pochta viruslari
1381. -:Fayl viruslari
1382. -:Protokol viruslari
1383. I:
1384. S: Qanday viruslar xavfli hisoblanadi?
1385. +:kompyuter ishlashida jiddiy nuqsonlarga olib keluvchi
1386. -:Jiddiy nuqsonlarga olib kelmaydigan ammo foydalanuvchini chalg'itadigan.
1387. -:Katta viruslar va odatda zararli dasturlar
1388. -:Passiv viruslar
1389. I:
1390. S: Rezident bo’lmagan viruslar qachon xotirani zararlaydi?
1391. +:Faqat faollashgan vaqtida
1392. -:Faqat o’chirilganda
1393. -:Kompyuter yoqilganda
1394. -:Tarmoq orqali ma’lumot almashishda
1395. I:
1396. S: Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan iborat?
1397. +:Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud
1398. -:Tarmoq chetki nuqtalari orasidagi xududning kengligi asosida qurilmalarholati
1399. -:Himoya vositalarining chegaralanganligi
1400. -:Himoyani amalga oshirish imkoniyati yo‘qligi va ma'lum protokollarning ishlatilishi
1401. I:
1402. S: Simmetrik shifrlashning noqulayligi – bu:
1403. +:Maxfiy kalitlar bilan ayirboshlash zaruriyatidir
1404. -:Kalitlar maxfiyligi
1405. -:Kalitlar uzunligi
1406. -:SHifrlashga ko‘p vaqt sarflanishi va ko'p yuklanishi
1407. I:
1408. S: Simsiz tarmoqlarni kategoriyalarini to’g’ri ko’rsating?
1409. +:Simsiz shaxsiy tarmoq (PAN), simsiz lokal tarmoq (LAN), simsiz regional tarmoq (MAN) va Simsiz global tarmoq (WAN)
1410. -:Simsiz internet tarmoq (IAN )va Simsiz telefon tarmoq (WLAN), Simsiz shaxsiy tarmoq (PAN) va Simsiz global tarmoq (WIMAX)
1411. -:Simsiz internet tarmoq (IAN) va uy simsiz tarmog’i
1412. -:Simsiz chegaralanmagan tarmoq (LAN), simsiz kirish nuqtalari
1413. I:
1414. S: Sub`ektga ma`lum vakolat va resurslarni berish muolajasi-bu:
1415. +:Avtorizatsiya
1416. -:Haqiqiylikni tasdiqlash
1417. -:Autentifikatsiya
1418. -:Identifikasiya
1419. I:
1420. S: Tarmoq operatsion tizimining to'g'ri konfiguratsiyasini madadlash masalasini odatda kim hal etadi?
1421. +:Tizim ma'muri
1422. -:Tizim foydalanuvchisi
1423. -:Korxona raxbari
1424. -:Operator
1425. I:
1426. S: Tarmoqlararo ekran texnologiyasi-bu:
1427. +:Ichki va tashqi tarmoq o’rtasida filtr va himoya vazifasini bajaradi
1428. -:Ichki va tashqi tarmoq o’rtasida axborotni o’zgartirish vazifasini bajaradi
1429. -:Qonuniy foydalanuvchilarni himoyalash
1430. -:Ishonchsiz tarmoqdan kirishni boshqarish}
1431. I:
1432. S: Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko’rsating?
1433. +:DDoS (Distributed Denial of Service) hujum
1434. -:Tarmoq hujumlari
1435. -:Dastur hujumlari asosidagi (Denial of Service) hujum
1436. -:Virus hujumlari}
1437. I:
1438. S: Uyishtirilmagan tahdid, ya’ni tizim yoki dasturdagi qurilmaning jismoniy xatoligi – bu…
1439. +:Tasodifiy tahdid
1440. -:Uyishtirilgan tahdid
1441. -:Faol tahdid
1442. -:Passiv tahdid
1443. I:
1444. S: Axborot xavfsizligi qanday asosiy xarakteristikalarga ega?
1445. +:Butunlik, konfidentsiallik, foydalana olishlik
1446. -:Butunlik, himoya, ishonchlilikni urganib chiqishlilik
1447. -:Konfidentsiallik, foydalana olishlik
1448. -:Himoyalanganlik, ishonchlilik, butunlik
1449. }
1450. I:
1451. S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa …. deb ataladi.
1452. +:"Sovuq saxiralash"
1453. -:"Issiq zaxiralash"
1454. -:"Iliq saxiralash"
1455. -:"To'liq zaxiralash"
1456. I:
1457. S: Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi …. deb ataladi?
1458. +:"Issiq zaxiralash"
1459. -:"Sovuq saxiralash"
1460. -:"Iliq saxiralash"
1461. -:"To'liq zaxiralash"
1462. I:
1463. S: Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang
1464. +:HandyBakcup
1465. -:Recuva, R.saver
1466. -:Cryptool
1467. -:Eset32
1468. I:
1469. S: O'chirilgan, formatlangan ma'lumotlarni tikovchi dasturni belgilang.
1470. +:Recuva, R.saver
1471. -:HandyBakcup
1472. -:Cryptool
1473. -:Eset32
1474. I:
1475. S: Virtuallashtirishga qaratilgan dasturiy vositalarni belgilang.
1476. +:VMware, VirtualBox
1477. -:HandyBakcup
1478. -:Eset32
1479. -:Cryptool
1480. I:
1481. S: Cloud Computing texnologiyasi nechta katta turga ajratiladi?
1482. +:3 turga
1483. -:2 turga
1484. -:4 turga
1485. -:5 turga
1486. I:
1487. S: O'rnatilgan tizimlar-bu…
1488. +:Bu ko'pincha real vaqt hisoblash cheklovlariga ega bo'lgan kattaroq mexanik yoki elektr tizimidagi maxsus funksiyaga ega, boshqaruvchidir
1489. -:Korxona ichki tarmog’iga ulangan korporativ tarmog’idan bo'ladigan hujumlardan himoyalash
1490. -:Korxona ichki tarmog’ini Internet global tarmog’idan ajratib qo’yish
1491. -:Bu ko'pincha global tizimda hisoblash cheklovlariga ega bo'lgan mexanik yoki elektr tizimidagi maxsus funksiyaga ega qurilmadir
1492. I:
1493. S: Axborotdan oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan?
1494. +:AQSH sog'liqni saqlash va insonlarga xizmat ko'rsatish vazirligi
1495. -:AQSH Mudofaa vazirligi
1496. -:O'zbekiston Axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi
1497. -:Rossiya kiberjinoyatlarga qarshu kurashish davlat qo'mitasi
1498. I:
1499. S: Axborotdan oqilona foydalanish kodeksi nechanchi yil ishlab chiqilgan?
1500. +:1973 yil
1501. -:1980 yil
1502. -:1991 yil
1503. -:2002 yil
1504. I:
1505. 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?
1506. +:Kiberetika
1507. -:Kiberhuquq
1508. -:Kiberqoida
1509. -:Kiberxavfsizlik
1510. I:
1511. S: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-…
1512. +:Kiberjinoyat
1513. -:Kibersport
1514. -:Kiberterror
1515. -:Hakerlar uyushmasi
1516. I:
1517. S: Tarmoqlararo ekran paket filtrlari qaysi sathda ishlaydi?
1518. +:Tarmoq sathida
1519. -:Ilova sathida
1520. -:Kanal sathida
1521. -:Fizik sathida
1522. I:
1523. S: Tarmoqlararo ekran ekspert paketi filtrlari qaysi sathda ishlaydi?
1524. +:Transport sathida
1525. -:Ilova sathida
1526. -:Kanal sathida
1527. -:Fizik sathida
1528. I:
1529. S: Spam bilan kurashishning dasturiy uslubida nimalar ko’zda tutiladi?
1530. +:Elektron pochta qutisiga kelib tushadigan ma’lumotlar dasturlar asosida filtrlanib cheklanadi
1531. -:Elektron pochta qutisiga kelib tushadigan spamlar me’yoriy xujjatlar asosida cheklanadi va bloklanadi
1532. -:Elektron pochta qutisiga kelib tushadigan spamlar ommaviy ravishda cheklanadi
1533. -:Elektron pochta qutisiga kelib spamlar mintaqaviy hududlarda cheklanadi
1534. I:
1535. S: Ma’lumotlarni yo’qolish sabab bo’luvchi tabiiy tahdidlarni ko’rsating
1536. +:Zilzila, yong‘in, suv toshqini va hak
1537. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
1538. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
1539. -:Qasddan yoki tasodifiy ma’lumotni o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani
1540. I:
1541. S: Ma’lumotlarni tasodifiy sabablar tufayli yo’qolish sababini belgilang
1542. +:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
1543. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
1544. -:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
1545. -:Zilzila, yong‘in, suv toshqini va hak
1546. I:
1547. S: Ma’lumotlarni inson xatosi tufayli yo’qolish sababini belgilang.
1548. +:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
1549. -:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
1550. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
1551. -:Zilzila, yong‘in, suv toshqini va hak
1552. I:
1553. S: Ma’lumotlarni g’arazli hatti harakatlar yo’qolish sababini ko’rsating.
1554. +:Tashkilotdagi muhim ma’lumotlarni modifikatsiyalanishi yoki o‘g‘irlanishi
1555. -:Quvvat o‘chishi, dasturiy ta’minot to‘satdan o‘zgarishi yoki qurilmani to‘satdan zararlanishi
1556. -:Ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
1557. -:Zilzila, yong‘in, suv toshqini va hak
1558. I:
1559. S: Kompyuterda hodisalar haqidagi ma’lumot qayerda saqlanadi?
1560. +:Hodisalar jurnaliga
1561. -:Operativ xotiraga
1562. -:Kesh xotiraga
1563. -:Vaqtinchalik faylga
1564. I:
1565. S: Internet orqali masofada joylashgan kompyuterga yoki tarmoq resurslariga DoS hujumlari uyushtirilishi natijasida..
1566. +:Foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan mahrum qilinadilar
1567. -:Foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzg’unchilarga etkaziladi
1568. -:Axborot tizimidagi ma’lumotlar bazalari o’g’irlanib ko’lga kiritilgach, ular yo’q qilinadilar
1569. -:Foydalanuvchilar axborotlariga ruxsatsiz o’zgartirishlar kiritilib, ularning yaxlitligi buziladi
1570. I:
1571. S: Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo’naltirilgan buzg’unchi bu - ... .
1572. +:Krakker
1573. -:Hakker
1574. -:Virus bot
1575. -:Ishonchsiz dasturchi
1576. I:
1577. S: Antivirus dasturiy vositalari viruslarni tahlil qilishiga ko'ra necha turga bo'linadi?
1578. +:2 turga: fayl Signaturaga va evristikaga asoslangan
1579. -:2 turga: faol va passiv
1580. -:2 turga: pulli va pulsiz
1581. -:2 turga: litsenziyali va ochiq
1582. I:
1583. S: "Parol', "PIN'" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?
1584. +:Foydalanish davrida maxfiylik kamayib boradi
1585. -:Parolni esda saqlash kerak bo'ladi
1586. -:Parolni almashtirish jarayoni murakkabligi
1587. -:Parol uzunligi soni cheklangan
1588. I:
1589. S: Yaxlitlikni buzilishi bu - …
1590. +:Soxtalashtirish va o’zgartirish
1591. -:Ishonchsizlik va soxtalashtirish
1592. -:Soxtalashtirish
1593. -:Butunmaslik va yaxlitlanmaganlik
1594. I:
1595. S: Tarmoqda joylashgan fayllar va boshqa resurslardan foydalanishni taqdim etuvchi tarmoqdagi kompyuter nima?
1596. +:Server
1597. -:Bulutli tizim
1598. -:Superkompyuter
1599. -:Tarmoq
1600. I:
1601. S: Tahdid nima?
1602. +:Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.
1603. -:Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa
1604. -:Bu riskni o‘zgartiradigan harakatlar bo‘lib
1605. -:Bu noaniqlikning maqsadlarga ta’siri
1606. I:
1607. S: Risk nima?
1608. +:Potensial kuchlanish yoki zarar
1609. -:Potensial foyda yoki zarar
1610. -:Tasodifiy taxdid
1611. -:Katta yo‘qotish
1612. I:
1613. S: Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi?
1614. +:Optik tolali
1615. -:O’rama juft
1616. -:Koaksial
1617. -:Telefon kabeli
1618. I:
1619. S: Nima uchun autentifikatsiyalashda parol ko’p qo’llaniladi?
1620. +:Sarf xarajati kam, almashtirish oson
1621. -:Parolni eslab qolish oson
1622. -:Parolni o’g’rishlash qiyin
1623. -:Serverda parollarni saqlash oson
1624. I:
1625. S: Elektron xujjatlarni yo’q qilish usullari qaysilar?
1626. +:Shredirlash, magnitsizlantirish, yanchish
1627. -:Yoqish, ko’mish, yanchish
1628. -:Shredirlash, yoqish, ko’mish
1629. -:Kimyoviy usul, yoqish.
1630. I:
1631. S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo‘ladi?
1632. +:Imzo qo‘yish va imzoni tekshirishdan
1633. -:Faqat imzo qo‘yishdan
1634. -:Faqat imzoni tekshirishdan
1635. -:Kalitlarni taqsimlashdan
1636. I:
1637. S: Elektron pochtaga kirishda foydalanuvchi qanday autetntifikasiyalashdan o’tadi?
1638. +:Parol asosida
1639. -:Smart karta asosida
1640. -:Biometrik asosida
1641. -:Ikki tomonlama
1642. I:
1643. S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Jazolar bosqichiga to‘g‘ri ta’rif berilgan.
1644. -: tashkilot o‘z siyosatini ishlab chiqishdan oldin o‘z aktivlari uchun risklarni baholashi shart
1645. -: tashkilot o‘z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o‘rnatilish shart
1646. -: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo‘shimcha kiritish jarayonida boshqaruvchi bo‘lishi shart
1647. +: ma’lum tashkilotlarda tashkilotlarda qat’iy siyosatlar mavjud. Agar xodimlar ushbu siyosatlarga amal qilmasa, ularga qarshi bir qancha choralar qo‘llaniladi.
1648. I:
1649. S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Xodimlarni o‘rgatish bosqichiga to‘g‘ri ta’rif berilgan.
1650. -: tashkilot o‘z siyosatini ishlab chiqishdan oldin o‘z aktivlari uchun risklarni baholashi shart
1651. -: tashkilot o‘z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o‘rnatilish shart
1652. -: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo‘shimcha kiritish jarayonida boshqaruvchi bo‘lishi shart
1653. +: xodimlarga tashkilot xavfsizlik siyosati davomli ravishda o‘rgatilishi shart
1654. I:
1655. S: Galstuk babochka usuli nima?
1656. +: Risklarni baholash usuli
1657. -: Risklarni qabul qilish usuli
1658. -: shifrlash algoritmi
1659. -: Risklarni hosil qilish usuli.
1660. I:
1661. S: Lotin alifbosida DADA so‘zini 3 kalit bilan shifrlagandan so‘ng qaysi so‘z hosil bo‘ladi. A=0, B=1….Z=25.
1662. +:GDGD
1663. -: NANA
1664. -: GPGP
1665. -: FDFD
1666. I:
1667. S: Lotin alifbosida NON so‘zini 3 kalit bilan shifrlagandan so‘ng qaysi so‘z hosil bo‘ladi. A=0, B=1….Z=25.
1668. -:GDGD
1669. -: NANA
1670. +: QRQ
1671. -: FDFD
1672. I:
1673. S: Fizik to‘siqlarni o‘rnatish , Xavfsizlik qo‘riqchilarini ishga olish, Fizik qulflar qo‘yishni amalga oshirish qanday nazorat turiga kiradi?
1674. +:Fizik nazorat
1675. -: Texnik nazorat
1676. -: Ma’muriy nazorat
1677. -: Tashkiliy nazorat
1678. I:
1679. 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?
1680. -: Fizik nazorat
1681. +:Texnik nazorat
1682. -: Ma’muriy nazorat
1683. -: Tashkiliy nazorat
1684. I:
1685. 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?
1686. -: Fizik nazorat
1687. -: Texnik nazorat
1688. +: Ma’muriy nazorat
1689. -: Tashkiliy nazorat
1690. I:
1691. S: Ikkilik sanoq tizimida qanday raqamlardan foydalanamiz?
1692. +: Faqat 0 va 1
1693. -: Faqat 1
1694. -: Faqat 0
1695. -: Barcha raqamlardan
1696. I:
1697. S: AES shifrlash algoritmi necha rounddan iborat
1698. +: 10, 12, 14
1699. -: 10,14,16
1700. -: 12,14,16
1701. -: 16
1702. I:
1703. S: Hodisalar daraxti usuli nima?
1704. +: Risklarni baholash usuli
1705. -: Risklarni qabul qilish usuli
1706. -: shifrlash algoritmi
1707. -: Risklarni hosil qilish usuli
1708. I:
1709. S: Yuliy Sezar ma’lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?
1710. +:3 taga
1711. -:4 taga
1712. -:2 taga
1713. -:5 taga
1714. I:
1715. S: WiMAX qanday simsiz tarmoq turiga kiradi.
1716. +: Regional
1717. -: Lokal
1718. -: Global
1719. -: Shaxsiy
1720. I:
1721. S: Wi-Fi necha Gs chastotali to'lqinda ishlaydi?
1722. +: 2.4-5 Gs
1723. -: 2.4-2.485 Gs
1724. -: 1.5-11 Gs
1725. -: 2.3-13.6 Gs
1726. I:
1727. S: Quyidagi parollarning qaysi biri “bardoshli parol”ga kiradi?
1728. +: Onx458&hdsh)
1729. +: 12456578
1730. +: salomDunyo
1731. +: Mashina777
1732. I:
1733. S: Parollash siyosatiga ko'ra parol tanlash shartlari qanday?
1734. +: 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.
1735. -: Kamida 6 belgi: katta xarflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak.
1736. -: 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. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid 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. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid 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. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 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 vositаlаri – bu ...

 Texnik qurilmаlаr, komplekslаr yoki tizimlаr yordаmidа ob’ektni himoyalаshdir

### 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. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid 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. Hаmmа nаrsа tа’qiqlаnаdi. Bu qаysi xаvfsizlik siyosаtigа hos?

 Pаrаnoid siyosаti (Pаrаnoid 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. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 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. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 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 vositаlаri – bu ...

 Texnik qurilmаlаr, komplekslаr yoki tizimlаr yordаmidа ob’ektni himoyalаshdir

### 

### 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. Dаstlаbki virus nechаnchi yildа yarаtilgаn?

 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