1. Axborot xavfsizligining asosiy maqsadlaridan biri-bu…

a) Obyektga bevosita ta’sir qilish
b) Axborotlarni o‘g‘irlanishini, yo‘qolishini, soxtalashtirilishini oldini olish
c) Axborotlarni shifrlash, saqlash, yetkazib berish
d) Tarmoqdagi foydalanuvchilarni xavfsizligini ta’minlab berish

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

a) 5 ta
b) 2 ta
c) 3 ta
d) 4 ta

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

a) axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
b) axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati;
c) axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati;
d) axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati;

4. Kriptografiya faninining asosiy maqsadi nima?

a) maxfiylik, yaxlitlilikni ta’minlash
b) ishonchlilik, butunlilikni ta’minlash
c) autentifikatsiya, identifikatsiya
d) ma’lumotlarni shaklini o‘zgartish

5. Kriptografiyada kalitning vazifasi nima?

a) Bir qancha kalitlar yig‘indisi
b) Matnni shifrlash va shifrini ochish uchun kerakli axborot
c) Axborotli kalitlar to‘plami
d) Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

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

a) simmetrik kriptotizimlar
b) assimetrik kriptotizimlar
c) ochiq kalitli kriptotizimlar
d) autentifikatsiyalash

7. Autentifikatsiya nima?

a) Ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi
b) Tizim me’yoriy 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

8. Identifikatsiya bu- …

a) Foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni
b) Ishonchliligini tarqalishi mumkin emasligi kafolati
c) Axborot boshlang‘ich ko‘rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o‘zgarishlar
d) Axborotni butunligini saqlab qolgan holda uni elementlarini o‘zgartirishga yo‘l qo‘ymaslik

9. Kriptobardoshlilik deb nimaga aytilladi?

a) kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi
b) axborotni qayta akslantirib himoyalash muammosi bilan shug‘ullanadi
c) kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi
d) axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

10. Kriptografiyada matn –bu..

a) alifbo elementlarining tartiblangan to‘plami
b) matnni shifrlash va shifrini ochish uchun kerakli axborot
c) axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam
d) kalit axborotni shifrlovchi kalitlar

11. Kriptotizimga qo‘yiladigan umumiy talablardan biri nima?

a) shifr matn uzunligi ochiq matn uzunligiga teng bo‘lishi kerak
b) shifrlash algoritmining tarkibiy elementlarini o‘zgartirish imkoniyati bo‘lishi lozim
c) ketma-ket qo‘llaniladigan kalitlar o‘rtasida oddiy va oson bog‘liqlik bo‘lishi kerak
d) maxfiylik o‘ta yuqori darajada bo‘lmoqligi lozim

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

a) Assi 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
b) Assimetrikrik tizimlarda k1=k2 bo‘ladi, ya’ni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi
c) Assimetrikrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma’lum bo‘ladi, ochiq kalitni esa faqat qabul qiluvchi biladi
d) Assimetrikrik kriptotizimlarda k1≠k2 bo‘lib, kalitlar hammaga oshkor etiladi
metrikrik kriptotizimlarda k1≠k2 bo‘lib, k1 ochiq kalit, k2 yopiq kalit deb yuritiladi, k1 bilan axborot shifrlanadi, k2 bilan esa deshifrlanadi
b) Assimetrikrik tizimlarda k1=k2 bo‘ladi, ya’ni k – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi
c) Assimetrikrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma’lum bo‘ladi, ochiq kalitni esa faqat qabul qiluvchi biladi
d) Assimetrikrik kriptotizimlarda k1≠k2 bo‘lib, kalitlar hammaga oshkor etiladi

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

a) login
b) parol
c) identifikatsiya
d) token

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

a) parol
b) login
c) identifikatsiya
d) maxfiy maydon

15. Ro‘yxatdan o‘tish-bu…

a) foydalanuvchilarni ro‘yxatga olish va ularga dasturlar va ma’lumotlarni ishlatishga huquq berish jarayoni
b) axborot tizimlari ob’yekt 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 ketma-ketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash

d) foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

16. Axborot qanday sifatlarga ega bo‘lishi kerak?

a) ishonchli, qimmatli va to‘liq
b) uzluksiz va uzlukli
c) ishonchli, qimmatli va uzlukli
d) ishonchli, qimmatli va uzluksiz

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

a) sirli yozuv
b) steganografiya
c) skrembler
d) shifr mashinalar

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

a) 4 ga
b) 3 ga
c) 2 ga
d) 5 ga

19. Shifrmatntni ochiq matntga akslantirish jarayoni nima deb ataladi?

a) Deshifrlash
b) Xabar
c) Shifrlangan xabar
d) Shifrlash

20. Risk-tushunchasi nima?

a) Belgilangan sharoitda tahdidning manbalarga bo‘lishi mumkin bo‘lgan zarar yetkazilishini kutish
b) Tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan
c) Shifrmatntni ochiq matntga akslantirish jarayoni
d) Kalitlarni generatsiya qilish usuli

21. Tahdid-tushunchasi nima?

a) 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

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
b) Ma’lumot boshqa formatga o‘zgartiriladi, biroq uni faqat maxsus shaxslar qayta o‘zgartirishi mumkin bo‘ladi
c) Ma’lumot boshqa formatga o‘zgartiriladi, barcha shaxslar kalit yordamida qayta o‘zgartirishi mumkin bo‘ladi
d) Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi

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

a) Kartografiya
b) Kriptoanaliz
c) Kriptologiya
d) Adamar usuli

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

a) {d, n} – yopiq, {e, n} – ochiq;
b) {d, e} – ochiq, {e, n} – yopiq;
c) {e, n} – yopiq, {d, n} – ochiq;
d) {e, n} – ochiq, {d, n} – yopiq;

25. Zamonaviy kriptografiya qanday bo‘limlardan iborat?

a) Simmetrik kriptotizimlar; Ochiq kalitli kriptotizimlar; Elektron raqamli imzo; Kalitlarni boshqarish
b) Elektron raqamli imzo; Kalitlarni boshqarish, Sertifikatlash, Shifrlash;
c) Simmetrik kriptotizimlar; Ochiq kalitli kriptotizimlar;
d) Simmetrik kriptotizimlar; Ochiq kalitli kriptotizimlar; Kalitlarni yaratish, Litsenziyalsh;

26. Shifr nima?

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

b) Kalitlarni taqsimlash usuli
c) Kalitlarni boshqarish usuli
d) Kalitlarni generatsiya qilish usuli

27. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

a) Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi
b) Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog‘langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi
c) Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat shifrlash mumkin
d) Ochiq kalitli kriptotizimlarda ma’lumotlarni faqat deshifrlash mumkin

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

a) Simmetrik algoritmlar
b) Assimmetrik algoritmlar
c) Xesh funksiyalar
d) Kodlash

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

a) Avtorizatsiya
b) Shifrlash
c) Identifikatsiya
d) Autentifikatsiya

30. Autentifikatsiya faktorlari nechta?

a) 4 ta
b) 3 ta
c) 5 ta
d) 6 ta

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

a) Biometrik autentifikatsiya
b) Biron nimaga egalik asosida
c) Biron nimani bilish asosida
d) Parolga asoslangan

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

a) Shifr matn uzunligi
b) Kriptobardoshlik
c) Shifrlash algoritmi
d) Texnika va texnologiyalar

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

a) 4 xil
b) 8 xil
c) 7 xil
d) 5 xil

34. Kiberjinoyat qanday turlarga bo‘linadi?

a) Ichki va tashqi
b) Faol va passiv
c) Asosiy va quyi
d) Xalqaro va milliy

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

a) 15.04.2022 y
b) 20.03.2021 y
c) 02.01.2000 y
d) 15.01.1995 y

36. Kiberjinoyatchilik bu –. . .

a) Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.
b) Kompyuter o‘yinlari
c) Faqat banklardan pul o‘g‘irlanishi
d) Autentifikatsiya jarayonini buzish

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

a) Axborotdan ruhsatsiz foydalanish

b) Zararkunanda dasturlar
c) An’anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili
d) Texnik vositalarning buzilishi va ishlamasligi

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

a) Axborotning konfedentsialligi
b) Foydalanuvchanligi
c) Ma’lumotlar butunligi
d) Ixchamligi

39. Biometrik autentifikatsiyalashning avfzalliklari-bu:

a) Bir marta ishlatilishi
b) Biometrik parametrlarning noyobligi
c) Biometrik parametrlarni o‘zgartirish imkoniyati
d) Autentifikatsiyalash jarayonining soddaligi

40. Simmetrik shifrlashning noqulayligi – bu:

a) Maxfiy kalitlar bilan ayirboshlash zaruriyatidir
b) Kalitlar maxfiyligi
c) Kalitlar uzunligi
d) Shifrlashga ko‘p vaqt sarflanishi va ko‘p yuklanishi

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 huquu 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. “Hamma narsa ta’qiqlanadi.” Bu qaysi xavfsizlik siyosatiga xos?

a) Ruxsat berishga asoslangan siyosat (Permissive Policy)
b) Paranoid siyosati (Paranoid Policy)
c) Ehtiyotkorlik siyosati (Prudent Policy)
d) Nomuntazam siyosat (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

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

82. 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

83. 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

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

a) Parol asosida
b) Smart karta asosida
c) Biometrik asosida
d) Ikki tomonlama

85. 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

86. 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

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

a) Sertifikatlari ro‘yxatga olish markazlari
b) Tegishli Vazirliklar
c) Axborot xavfsizligi markazlari
d) Davlat Hokimiyati

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

a) Autentifikatsiya

b) Identifikatsiya
c) Avtorizatsiya
d) Ma’murlash

89. 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

90. 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

91. 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

92. 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

93. 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

94. 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

95. 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,

96. 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.

97. 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

98. 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

99. 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

100. 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.

101. 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

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

a) 8 ta
b) 7 ta
c) 6 ta
d) 5 ta

103. 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

104. Kiberxavfsizlik arxitekturasi nechta sathga ajratiladi?

a) 3ta
b) 2 ta
c) 4 ta
d) 5 ta

105. 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.

106. 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.

107. 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.

108. 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.

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

a) Kriptotizim
b) Deshifrlash
c) Rasshifrovkalash
d) Shifrlash

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

a) Kriptotizim
b) Kalit
c) Rasshifrovkalash
d) Shifrlash

111. "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.

112. "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

113. "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

114. .... – 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

115. .... 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

116. “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.

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

a) Foydalanishni boshqarish
b) Tarmoqni loyihalash
c) Foydalanish
d) Identifikatsiya

118. “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

119. “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

120. “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

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

a) UDP
b) HTTP
c) TCP
d) FTP

122. ….. 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

123. 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

124. “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

125. 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"

126. 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"

127. 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"

128. 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;

129. 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;

130. 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

131. 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

132. 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

133. Antivirus dasturlarini ko‘rsating.

a) Drweb, Nod32, Kaspersky
b) arj, rar, pkzip, pkunzip
c) winrar, winzip, winarj
d) pak, lha

134. Antiviruslar viruslarni asosan qanday usulda aniqlaydi?

a) Signaturaga asoslangan
b) Anomaliyaga asoslangan
c) O‘zgarishni aniqlashga asoslangan
d) Defragmentatsiya qilish

135. 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

136. 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

137. 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

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

a) Ikkita kalit
b) Bitta kalit
c) Uchta kalit
d) Foydalanuvchi identifikatori

139. 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

140. 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

141. 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

142. 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

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

a) Korporativ va umumfoydalanuvchi
b) Regional, korporativ
c) Lokal, global
d) Shaharlararo, lokal, global

144. Axborot paketlarini qachon ushlab qolish mumkin?

a) Aloqa kanallari orqali uzatishda
b) Xotira qurilmalarida saqlanayotganda
c) Kompyuter ishga tushganda
d) Ma’lumotlar nusxalanayotganda

145. 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

146. 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

147. Axborot xavfsizligi siyoatining necha xil turi bor?

a) 3
b) 4
c) 5
d) 2

148. 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.

149. 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

150. 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

151. 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

152. 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

153. 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

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

a) Tahdid
b) Zaiflik
c) Hujum
d) Butunlik

155. Axborotning eng kichik o‘lchov birligi nima?

a) bit
b) kilobayt
c) bayt
d) kilobit

156. Axborot tizimlari xavfsizligining auditi-bu…

a) Axborot tizimlarining himoyalanishining joriy holati, tizim haqida obyektiv ma’lumotlarni olish va baholash
b) Ma`lumotlarini tahlillash va chora ko‘rishni tizim haqida subyektiv ma’lumotlarni olish va baholashni tahlil qiladi
c) Ma`lumotlarini tarqatish va boshqarish

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

157. TrueCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi?

a) AES, Serpent va Twofish
b) Serpent, RSA
c) El-Gamal, Twofish
d) DES

158. "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

159. "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

160. 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

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

a) Konfidentsiallikni
b) Yaxlitlikni
c) Maxfiylikni
d) O‘zgarmaslikni

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

a) Yaxlitligi
b) Maxfiyligi
c) Xavfsizligi
d) Konfidentsialligi

163. BiBa modeli qaysi modelning keygaytirilgan varianti hisoblanadi?

a) Bell-Lapadula modeli
b) RBAC
c) MAC
d) ABAC

164. 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

165. 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

166. 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.

167. …-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

168. Bulutli texnologiyalarda PaaS nimani ifodalaydi?

a) Platforma sifatida
b) Servis sifatida
c) Ma'lumot sifatida
d) Prizentatsiya sifatida

169. 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

170. Cloud Computing texnologiyasi nechta katta turga ajratiladi?

a) 3 turga
b) 2 turga
c) 4 turga
d) 5 turga

171. 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

172. Dasturiy shifrlash vositalari necha turga bo‘linadi?

a) 4
b) 3

c) 5
d) 6

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

a) Krakker
b) Hakker
c) Virus bot
d) Ishonchsiz dasturchi

174. 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

175. 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

176. 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

177. 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

178. 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

179. 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

180. 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

181. 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

182. 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

183. Faollashish prinspiga ko‘ra viruslar turlari?

a) Rezident, Norezident
b) Dasturiy, Makroviruslar, multiplatformali viruslar
c) Virus parazit, Virus cherv
d) Shifrlangan, shifrlanmagan, Polimorf

184. 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)

185. 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)

186. 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