1. Elektron axborot saqlovchilardan qayta foydalanishli ma’lumotlarni yo’q qilish usullari orasidan eng ishonchlisini aniqlang.
2. Formatlash
3. Delete buyrug’I yordamida o’chirish
4. Shift+Delete buyrug’I yordamida o’chirish
5. ***Takroriy qayta yozish***
6. 5 XOR 8 =? Natijani hisoblang.
7. ***13***
8. 10
9. 11
10. 40
11. Agar a – ochiq kalit, b – shaxsi kalit, H – xabar, X() – xesh funksiya bo’lsa Sign() – imzolash funksiyasi uchun asosiy parametrlariga asoslangan ko’rinishini ko’rsating.
12. Sign(X(H), a)
13. Sign(H, a)
14. Sign(H, b)
15. ***Sign(X(H), b)***
16. Ma’lumotni to’liq qayta tiklash qachon samarali amalga oshiriladi?
17. Formatlash asosida ma’lumot o’chirilgan bo’lsa
18. ***Saqlagichda ma’lumot qayta yozilmagan bo’lsa***
19. Ma’lumotni o’chirish Delete buyrug’I bilan amalga oshirilgan bo’lsa
20. Ma’lumotni o’chirish Shift+Delete buyrug’I bilan amalga oshirilgan bo’lsa
21. …… - ushbu zaxiralashda tarmoqqa bog’lanish amalga oshiriladi. Ushbu zaxiralashda, tizim yangilanishi davomiy yangilanishni qabul qilish uchun ulanadi.
22. Issiq zaxiralash
23. Ichki zaxiralash
24. ***Iliq zaxiralash***
25. Sovuq zaxiralash
26. Agar biror xesh funksiyaga kiruvchi ma’lumot uzunligi 512 bit bo’lganida, chiquvchi qiymat 128 bitga teng bo’lsa, shu funksiyaga 1024 bit ma’lumot kiritilganida chiqish biti necha bitga teng bo’ladi?
27. Hisoblash uchun shartlar yetarli emas
28. ***128***
29. 64
30. 256
31. Sotsial injeneriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan?
32. Biometrik autentifikatsiya
33. Ko’z qorachig’iga asoslangan autentifikatsiya
34. Tokenga asoslagan autentifikatsiya
35. ***Parolga asoslangan autentifikatsiya***
36. 2 XOR 6 = ? Natijani hisoblang.
37. ***4***
38. 6
39. 8
40. 12
41. VPNning texnik yechim arxitekturasiga ko’ra turlari keltirilgan qatorni toping.
42. Kanal sathidagi VPN; tarmoq sathidagi VPN; seans sathidagi VPN
43. Dasturiy ko’rinishdagi VPN; maxsus shifrlash protsessoriga ega apparat vosita ko’rinishidagi VPN
44. Marshuritizator ko’rinishidagi VPN; tarmoqlararo ko’rinishidagi VPN
45. ***Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN***
46. 6 XOR 6 = ? Natijani hisoblang.
47. ***0***
48. 6
49. 12
50. 36
51. Parolga xos bo’lmagan xususiyatni ko’rsating.
52. Klaviatura orqali barcha kiritiluvchi qiymatlarni qabul qiladi
53. PIN kodni parolni xususiy holati sifatida qarash mumkin
54. Ixtiyoriy uzunlikda bo’lishi mumkin
55. ***Faqat pechat qilinuvchi belgilarni qabul qiladi***
56. Tarmoqlararo ekran vositasi bajarilishiga ko’ra qanday turlarga bo’linadi?
57. Paket filterlari – tarmoq sathida ishlaydi, ekspert paketi filterlari – transport sathida ishlaydi; ilova proksilari – ilova sathida ishlaydi
58. Yagona tarmoq himoyasi sxemasi; himoyalangan yopiq va himoyalanmagan ochiq tarmoq segmentli sxema; bo’lingan himoyalangan yopiq va ochiq segmentli tarmoq sxemasi
59. ***Apparat-dasturiy: Dasturiy***
60. Protokol holatini nazoratlash: vositachi yordamida(proksi)
61. GSM tarmog’ida ovozli so’zlashuvlarni shifrlash algoritmi bu?
62. RSA
63. ***A5/1***
64. ГОСТ
65. DES
66. Xavfsizlik siyosati xususiyatlari keltirilgan qatorni ko’rsating.
67. Tushunarli bo’lishi, amaliy bo’lishi
68. ***Barcha javoblar to’g’ri***
69. Qisqa va aniq foydalanuvchan bo’lishi
70. Iqtisodiy asoslangan bo’lishi
71. Biba modelida birinchi ob’ektning ishonchlilik darajasi I(01) ga va ikkinchi ob’ektning ishonchlilik darajasi I(02) ga teng bo’lsa, ushbu ikkita ob’ektdan iborat bo’lgan uchinchi ob’ektning ishonchlilik darajasi nimaga teng? Bu yerda I(01)>I(02).
72. ***I(02)***
73. Berilgan shartlar yetarli emas
74. I(01) va I(02) ga bog’liq emas
75. I(01)
76. Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi?
77. Antivirus
78. Router
79. ***Tarmoqlararo ekran***
80. Virtual himoyalangan tarmoq
81. Elektron raqamli imzo keltirilganlardan qaysi xususiyatni ta’minlamaydi?
82. Yaxlitlik
83. Qalbakilashtirishdan himoya
84. ***Konfidensiallik***
85. Rad etishdan himoya
86. Zudlik bilan chora ko’rish talab etilmasada, qisqa vaqtda qarshi harakatlarni qo’llash zarur; Riskni yetarlicha past darajagacha tushurish uchun imkoni boricha nazorati amalga oshirish kerak. Mazkur harakatlar riskning qaysi darajasi uchun?
87. Quyi
88. Barcha
89. Yuqori
90. ***O’rta***
91. Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo’shimcha apparat va dasturiy vositani talab qiladi?
92. USB disklar
93. Ko’chma qattiq disklar
94. CD/DVD disklar
95. ***Lentali disklar***
96. Eng zaif simsiz tarmoq protokolini ko’rsating.
97. WPA3
98. ***WEP***
99. WPA2
100. WPA
101. Parolga “tuz”ni qo’shib xeshlashdan maqsad?
102. ***Tahdidchi ishini oshirish***
103. Murakkab parol hosil qilish
104. Yana bir maxfiy parametr kiritish
105. Murakkab xesh qiymat qiymat hosil qilish
106. *(Bob-), (Alisa,rw), (Sem,rw), (buxgalteriyaga oid dastur,rw).* Ushbu qoida quyidagilardan qaysi biriga tegishli?
107. Biba modeli
108. Imtiyozlar ro’yhati yoki C-list
109. ***Foydalanishni boshqarish ro’yhati yoki ACL***
110. Foydalanishni boshqarish matritsasi
111. Jumlani to’ldiring. …… - muhim bo’lgan avborot nusxalash yoki saqlash jarayoni bo’lib, bu ma’lumot yo’qolgan vaqtda qayta tiklash imkoniyatini beradi.
112. VPN
113. Kriptogtafik himoya
114. ***Ma’lumotlarni zaxira nusxalash***
115. Tarmoqlararo ekran
116. Sub’ekt.lavozimi=Vrach & muhit.vaqt >= 8:00 & muhit.vaqt <= 18:00. Ushbu keltirilgan shart qaysi foydalanishni boshqarish usuliga tegishli?
117. Rolga asoslangan foydalanishni boshqarish
118. Mandatli foydalanishmi boshqarish
119. ***Attributga asoslangan foydalanishni boshqarish***
120. Diskretsion foydalanishni boshqarish
121. Trafik orqali axborotni to’plashga harakat qilish razvedka hujumlarining qaysi turida amalga oshiriladi?
122. Lug’atga asoslangan
123. ***Passiv***
124. DNS izi
125. Aktiv
126. Modul arifmetikasida mod7 bo’yicha 4 soniga teskari bo’lgan sonni toping?
127. ¼
128. 2
129. 4
130. ***7***
131. A5/1 shifrlash algoritmida registrlar siljiganidan keying holat: x18=0, y21=1 va z22=1 ga teng bo’lsa, hosil bo’lgan psevdotasodifiy qiymatni ko’rsating.
132. ***0***
133. 11
134. 1
135. 110
136. Zaxiralashni amalga oshirishda inson ishtirokini talab etadi; Tabiiy-ofatlarga yoki o’g’irlashga moyil. Ushbu xususiyat qaysi zaxira nusxalash manziliga tegishli?
137. Bulutli tizmda zaxiralash
138. Barcha javoblar to’g’ri
139. Tashqi (offsite) zaxiralash
140. ***Ichki (onsite) zaxiralash***
141. Resurslardan foydalanish usuliga ko’ra kompyuter viruslari qanday turlarga bo’linadi?
142. Shifrlangan, shifrlanmagan va polimorf
143. Dasturiy, yuklanuvchi, makroviruslar va ko’p platformali
144. Resident va norezident
145. ***Virus-parazitlar va virus-chervlar***
146. Risk ta’sirini kamaytirish uchun profilaktika choralarini ko’rish zarur. Mazkur harakatlar riskning qaysi darajasi uchin?
147. Barcha
148. ***Quyi***
149. O’rta
150. Yuqori
151. TCP/IP modelidagi kanal sathi OSI modelidagi qaysi sathlarga mos keladi?
152. Tarmoq va kanal
153. Kanal
154. ***Fizik va kanal***
155. Fizik
156. “Kompilyator foydalanuvchining imtiyoziga ko’ra ish ko’rish o’rniga o’zining imtiyoziga asosan ish ko’rishi” klassik xavfsizlik sohasida nima deb yuritiladi?
157. Donadorlik muammosi
158. Klassifikatsiyalashdagi muammo
159. Cheklanishdagi muammo
160. ***Tartibsiz yordamchi muammosi***
161. 2 XOR 4 = ? Natijani hisoblang.
162. ***6***
163. 4
164. 2
165. 8
166. 5 XOR 8 = ? Natijani hisoblang.
167. 10
168. ***13***
169. 40
170. 12
171. Markaziy xab yoki tugun orqali tarmoqni markazlashgan holda boshqarish qaysi tarmoq topologiyasida amalga oshiriladi?
172. Mesh
173. Xalqa
174. Shina
175. ***Yulduz***
176. Yaratishda psevdotasofiy sonlar generatoriga asoslanuvchi kriptografik shifrlash usuli bu?
177. Ochiq kalitli
178. Assimmetrik
179. Simmetrik blokli
180. ***Simmetrik oqimli***
181. 4 XOR 4 = ? Natijani hisoblang.
182. ***0***
183. 8
184. 16
185. 4
186. Elektron raqamli imzo muolajalarini ko’rsating.
187. Imzoni shakllantirish va xeshlash
188. Imzoni xeshlash va xesh matni deshifrlash
189. Shifrlash va deshifrlash
190. ***Imzoni shakllantirish va imzoni tekshirish***
191. Foydalanuvchining tizimga muvaffaqiyatli urinishi Windows OT da qanday audit hodisasi sifatida qayd etiladi?
192. Muvaffaqiyatsiz audit
193. Ogohlantirish
194. Xatolik
195. ***Muvaffaqiyatli audit***
196. Ushbu hujumda foydalanuvchilarning akkauntlari bloklangani va kredit karta ma’lumotlari blokdan chiqarilishi kerakli to’g’risidagi ma’lumot foydalanuvchi electron pochtalariga yuboriladi. Gap qaysi ijtimoiy injeneriya turi haqida bormoqda?
197. ***Phishing***
198. Spoofing
199. Protexting
200. Barcha javoblar to’g’ri
201. Ma’lumotni zaxira nusxalash nima uchun potensial tahdidlarni paydo bo’lish ehtimolini oshiradi?
202. ***Tahdidchi uchun nishon ko’payadi***
203. Ma’lumot yo’qolgan taqdirda ham tiklash imkoniyati mavjud bo’ladi
204. Saqlanuvchi ma’lumot hajmi ortadi
205. Ma’lumotni butunligi ta’minlanadi
206. Manbaga zarar keltiradigan ichki va tashqi zaiflik ta’sirida tahdid qilish ehtimoli bu?
207. Hujum
208. Zaiflik
209. ***Risk***
210. Tahdid
211. RSA algoritmida ochiq kalit e=5, N=35 ga teng bo’lsa, M=3 ga teng ochiq matnni shifrlash natijasini ko’rsating.
212. 35
213. 7
214. 5
215. 33
216. RAID 3 texnologiyasing vazifasi –
217. ***Diskni navbatlanishi va xatolikni nazoratlash***
218. Bloklarni navbatlash va akslantirish
219. Diskni navbatlanishi
220. Diskni akslantirish
221. RSA algoritmida p=3, q=11 bo’lsa, N sonidan kichik va u bilan o’zaro tub bo’lgan sonlar miqdorini ko’rsating.
222. 14
223. 33
224. ***20***
225. 12
226. Resursni va harakatni kim bajarayotgani to’g’risidagi holatlar “AGAR, U HOLDA” dan tashkil topgan qoidalarga asoslanadi. Gap qaysi foydalanishni boshqarish usuli haqida bormoqda?
227. DAC
228. MAC
229. RBAC
230. ***ABAC***
231. Ichki yoki tashqi majburiyatlar natijasida tahdid yoki hodisalarni yuzaga kelishi, yo’qotilishi yoki boshqa salbiy ta’sir ko’rsatishi mumkin bo’lgan voqea bu?
232. ***Risk***
233. Hujum
234. Tahdid
235. Zaiflik
236. Jumlani to’ldiring. Tarmoqlararo ekranning vazifasi …
237. Tarmoq hujumlarini aniqlash
238. Tarmoqdagi xabarlar oqimini uzish va ulash
239. ***Ishonchli va ishonchsiz tarmoqlar orasida ma’lumotlarga kirishni boshqarish***
240. Trafikni taqiqlash
241. Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan?
242. Apparat nazoratlash
243. ***Ma’muriy nazoratlash***
244. Texnik nazoratlash
245. Fizik nazoratlash
246. RSA algoritmida p=7, q=5 bo’lsa, N sonidan kichik va u bilan o’zaro tub bo’lgan sonlar miqdorini ko’rsating.
247. ***24***
248. 35
249. 12
250. 60
251. Foydalanishni boshqarish matritsasi ustunlar bo’yicha bo’linsa … hosil bo’ladi.
252. ***Foydalanishni boshqarish ro’yhati yoki ACL***
253. Foydalanishni boshqarish matritsasi
254. Imtiyozlar ro’yhati yoki C-list
255. Biba modeli
256. Faraz qilaylik tizimdagi barcha fayllarni xeshlab, xesh qiymatlari xavfsiz manzilga saqlangan bo’lsin. U holda vaqti-vaqti bilan ushbu faylning xesh qiymatlari qaytadan xeshlanadi va dastlabki holatdagilari bilan taqqoslanadi. Agar faylning bir yoki bir nechta bitlari oz’garishga uchragan bo’lsa, u holda xesh bir-biriga mos kelmaydi va natijada uni virus tomonidan zararlangan deb qarash mumkin. Bu zararli dasturiy vositalarmi aniqlashning qaysi usuliga misol bo’ladi?
257. Anomaliyaga asoslangan
258. Signaturaga asoslangan
259. ***O’zgarishni aniqlashga asoslangan***
260. Barchasiga
261. Parollarni saqlashda nega shifrlashning o’rniga xeshlash amalidan foydalaniladi?
262. Shifrlash algoritmlari xavfsiz emas
263. Shifrlash algoritmlari tezkor emas
264. Xesh funksiyalari xavfsiz
265. ***Shifrlash kalitini saqlash zaruriyati mavjud***
266. Modul arifmetikasida mod7 bo’yicha 5 soniga teskari bo’lgan sonni toping?
267. ***3***
268. 35
269. 2
270. 5/7
271. Voqea sodir bo’lish ehtimoli va ushbu hodisaning axborot texnologiyalari aktivlariga ta’siri bu?
272. Hujum
273. Tahdid
274. Zaiflik
275. ***Risk***
276. Kriptografiya so’ziga berilgan to’g’ri tavsifni toping?
277. Maxfiy shifrlarni yaratish va buzish fani va san’ati
278. ***Maxfiy shifrlarni yaratish fani va san’ati***
279. Axborotni himoyalash fani va san’ati
280. Maxfiy shifrlarni buzish fani va san’ati
281. Asosiy maqsad ma’lumotni maxfiyligini ta’minlash bo’lgan jarayonni ko’rsating?
282. Dekodlash
283. Kodlash
284. ***Shifrlash***
285. Deshifrlash
286. Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting.
287. Almashib bo’lmaslik
288. Doimo esda saqlash zaruriyati
289. ***Doimo xavfsiz saqlab olib yurish zaruriyati***
290. Qalbakilashtirish muammosi mavjudligi
291. Agar d – ochiq kalit, e – shaxsi kalit, X – xabar, H() – xesh funksiya bo’lsa Sign() – imzolash funksiyasi uchun asosiy parametrlariga asoslangan ko’rinishini ko’rsating.
292. Sign(X, d)
293. Sign(X, e)
294. Sign(H(X), d)
295. ***Sign(H(X), e)***
296. RSA algoritmida p=5, q=11 bo’lsa, N sonidan kichik va u bilan o’zaro tub bo’lgan sonlar miqdorini ko’rsating.
297. 55
298. 10
299. 11
300. ***40***
301. Paydo bo’lishi tasodifiy, qasddan yoki boshqa harakatning ta’sirida bo’lishi mumkin bo’lgan hodisa bu?
302. ***Tahdid***
303. Aktiv
304. Hujum
305. Zaiflik
306. Risklarga qarshi zudlikda chora ko’rish zarur; riskni yetarlicha past darajagacha tushirish uchun nazoratlash vositalarini aniqlash va o’rnatish kerak. Mazkur harakatlar riskning qaysi darajasi uchun?
307. O’rta
308. ***Yuqori***
309. Quyi
310. Barcha
311. Ushbu hujumda qurbonni shubhalanmasligi uchun tegishli tayyorgarlik ko’riladi: tug’ilgan kun, INN, passport raqami yoki hisob raqamining oxirgi belgilari kabi ma’lumotlar topiladi. Gap qaysi ijtimoiy injineriya turi haqida bormoqda?
312. Barcha javoblar to’g’ri
313. Protexting
314. ***Phishing***
315. Spoofing
316. Turli xil psixologik usullar va firibgarlik amaliyoting turlari bo’lib, uning maqsadi firibgarlik yo’li bilan shaxs to’g’risida maxfiy ma’lumotlarni olishdan iborat. Gap nima haqida bormoqda?
317. Kibernetika
318. Kiberxavfsizlik
319. ***Ijtimoiy injeneriya***
320. Kiberjinoyatlar
321. A5/1 oqimli shifrlash algoritmida maj(1,1,1) ga bo’lsa, qaysi registorlar siljiydi?
322. Y
323. ***X,Y,Z***
324. X,Y
325. X,Z
326. Ochiq kalitli kriptotizimda ma’lumotga imzo qo’yish qaysi kalit yordamida amalga oshiriladi?
327. Yuboruvchining ochiq kaliti
328. Qabul qiluvchining ochiq kaliti
329. Yuboruvchining shaxsiy kaliti
330. Qabul qiluvchining shaxsiy kaliti
331. Modul arifmetikasida mod11 bo’yicha 3 soniga teskari bo’lgan sonni toping?
332. ***5***
333. 1/11
334. 4
335. 1/3
336. A5/1 algoritmidagi Y registor uzunligi nechiga teng?
337. 21
338. ***22***
339. 23
340. 19
341. RSA algoritmidagi ochiq va shaxsiy kalitlar uchun qanday munosabat o’rinli?
342. Ochiq va shaxsiy kalitlar mod(p\*q) bo’yicha o’zaro teskari
343. Ochiq va shaxsiy kalitlar uchun biror munosabat o’rinli emas
344. Ochiq va shaxsiy kalitlar modN bo’yicha o’zaro teskari
345. Ochiq va shaxsiy kalitlar modϕ(N) bo’yicha o’zaro teskari
346. Eng kam vaqtda ma’lumotni tiklash imkoniyatiga ega usul bu?
347. ***Differensial zaxiralash***
348. O’sib boruvchi zaxiralash
349. To’liq zaxiralash
350. Ichki zaxiralash
351. Qurbon kompyuteridagi ma’lumotni shifrlab, uni deshifrlash uchun to’lovni amalga oshirishni talab qiluvchi zararli dastur bu-?
352. Rootkits
353. Mantiqiy bombalar
354. Spyware
355. ***Ransomware***
356. Tarmoqlararo ekran vositasi OSI modeling funksional sathlari bo’yicha qanday turlarga bo’linadi?
357. ***Paket filterlari – tarmoq sathida ishlaydi; ekspert paketi filterlari – transport sathida ishlaydi; ilova proksilari – ilova sathida ishlaydi***
358. Protokl holatini nazoratlash; vositachi yordamida nazoratlash (proksi)
359. Apparat-dasturiy; dasturiy
360. Yagona tarmoq himoyasi sxemasi; himoyalangan yopiq va himoyalanmagan ochiq tarmoq segmentli sxema; bo’lingan himoyalangan yopiq va ochiq segmentli tarmoq sxemasi
361. Ochiq matn qismlarini takroriy shifrlovchi algoritmlar bu –
362. Blokli shifrlar
363. Ochiq kalitli shifrlar
364. Asimmetrik shifrlar
365. Oqimli shifrlash
366. Ma’lumot shifrlansa, natijasi …. bo’ladi.
367. No’malum
368. Ochiq matn
369. Kod
370. ***Shifrmatn***
371. Tarmoqdagi barcha tugunlarni o’zaro bog’laydi. Gap qaysi topologiya haqida bormoqda?
372. ***Halqa***
373. Yulduz
374. Shina
375. Daraxt
376. Agar simmetrik oqimli shifrlash algoritmida kiritilgan ochiq matn uzunligi 256 bitga teng bo’lsa, shifrmatn uzunligi necha bit bo’ladi?
377. 128
378. ***256***
379. 4
380. 64
381. Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu?
382. Identifikatsiya
383. Autentifikatsiya
384. Ro’yxatga olish
385. ***Avtorizatsiya***
386. Parollar 10 xonali uzunlikka va har bir xonasi uchun 16ta turli belgilar bo’lishi mumkin bo’lgan jami parollar soni nechta?
387. 26
388. 160
389. 10^16
390. ***16^10***
391. Shaxsni kimdir deb davo qilish jarayoni bu?
392. Ruxsatlarni nazoratlash
393. Avtorizatsiya
394. Autentifikatsiya
395. ***Identifikatsiya***
396. VPNni OSI modelining “ishchi sathlari” ga ko’ra turlari keltirilgan qatorni aniqlang?
397. ***Kanal sathidagi vpn; tarmoq sathidagi vpn; seans sathidagi vpn***
398. Dasturiy ko’rinishdagi vpn; maxsus shifrlash protsessoriga ega apparat vosita ko’rinishidagi vpn
399. Korporativ tarmoq ichidagi vpn; masofadan foydalaniluvchi vpn; korporativ tarmoqlararo vpn
400. Marshuritizator ko’rinishidagi vpn; tarmoqlararo ekran ko’rinishidagi vpn
401. Asosiy fayl tizimining ustida joylashgan kriptografik fayl tizimidan foydalaniladi. Gap qaysi shifrlash usuli xususida bormoqda?
402. Dasturiy shifrlash
403. ***Faylni shifrlash***
404. Apparat shifrlash
405. Diskni shifrlash
406. Yo’q qilish usullari orasidan ekologik jihatdan ma’qullanmaydigan va maxsus joy talab qiladigan usul qaysi?
407. Ko’mish
408. ***Yoqish***
409. Kimyoviy ishlov berish
410. Maydalash
411. Qaysi akslantirishda ochiq matndagi belgilarning takrorlanish chastotasi shifrmatndagi belgilarda ham bir xil bo’ladi?
412. Bir alifboli o’rniga qo’yish
413. Gammalash
414. Qo’shish
415. ***O’rin almashtirish***
416. Blokli simmetrik shifrlashda shifrmatndagi bir bitning o’zgarishi deshifrlangan matndagi necha bitning o’zgarishiga olib keladi?
417. Buni aniqlash imkonsiz
418. 1
419. Barchasiga
420. Kamida bir blokiga
421. [www.PayPai.com](http://www.PayPai.com) manzili [www.PayPal.com](http://www.PayPal.com) manzili sifatida yuboriladi. Bu qaysi turdagi hujumga misol bo’ladi?
422. Protexting
423. ***Phishing***
424. Spoofing
425. Barcha javoblar to’g’ri
426. Zaxira nusxalash manzillarini ko’rsating.
427. To’liq, differensial va o’sib boruvchi zaxiralash
428. Barcha javoblar to’g’ri
429. Issiq, sovuq va iliq zaxiralash
430. ***Ichki, tashqi va bulutda zaxiralash***
431. AGAR talabgor boshqaruvchi bo’lsa, U HOLDA maxfiy ma’lumotni o’qish/yozish huquqi berilsin. Bu qaysi foydalanishni boshqarish usuliga misol bo’ladi?
432. DAC
433. RBAC
434. MAC
435. ***ABAC***
436. A5/1 oqimli shifrlash algoritmining bir siklda kamida nechta registr siljiydi?
437. 3
438. 1
439. 0
440. ***2***
441. Bir-biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi bu?
442. Tarmoq topologiyasi
443. ***Kompyuter tarmog’i***
444. Kompyuter topologiyasi
445. Tarmoq arxitekturasi
446. Subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim etish jarayoni bu?
447. Avtorizatsiya
448. ***Identifikatsiya***
449. Ruxsatlarni nazoratlash
450. Autentifikatsiya
451. Foydalanishni boshqarishning qaysi usulida asosiy g’oya tizimning ishlash logikasini tashkilotdagi kadrlar vazifasiga yaqinlashtirishga harakat qilinadi?
452. DAC
453. ***RBAC***
454. MAC
455. ABAC
456. Yong’inga qarshi kurashishning aktiv usuli to’g’ri ko’rsatilgan javobni toping.
457. Minimal darajada yonuvchan materiallardan foydalanish, qo’shimcha etaj va xonalar qurish
458. Binoga istiqomat qiluvchilarni yong’in sodir bo’lganda qilinishi zarur bo’lgan ishlar bilan tanishtirish
459. Yetarli sondagi qo’shimcha chiqish yo’llarini mavjudligi
460. ***Tutunni aniqlovchilar, alangani aniqlovchilar va issiqlikni aniqlovchilar***
461. A5/1 shifrlash algoritmida registrlar siljiganidan keying holat: x18=1, y21=1 va z22=1 ga teng bo’lsa, hosil bo’lgan psevdotasodifiy qiymatni ko’rsating.
462. 0
463. 11
464. 111
465. ***1***
466. Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko’rsating.
467. Parollar lug’atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydalanish asisida hujum
468. Parollar lug’atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararki dasturladan foydalanish asosida hujum
469. Fizik o’g’irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar
470. Fizik o’g’irlash, yelka orqali qarash hujumi, zararli dasturlardan foydalanishga asoslangan hujumlar
471. Seans sathidagi VPN qaysi protocol asosida quriladi?
472. IPsec
473. PPTP
474. L2F
475. ***TLS***
476. RSA algoritmida p=7, q=11, e=7 ga teng bo’lsa, shaxsiy kalitni hisoblang.
477. ***43***
478. 7
479. 77
480. 11
481. Qaysi himoya vositasi mavjud IP – paketni to’liq shifrlab, unga yangi IP sarlavha beradi?
482. Router
483. Tarmoqlararo ekran
484. ***VPN***
485. Antivirus
486. Faqat simsiz tarmoqlarga xos bo’lgan zaifliklarni ko’rsating?
487. Zararli dasturlardan foydalanishga asoslangan hujumlarni mavjudliligi
488. ***Nazoratlanmaydigan hududni har doim mavjudligi***
489. Xizmat ko’rsatishdan voz kechish hujumini mavjudligi
490. O’rtaga turgan odam hujumini mavjudligi
491. Juda ahamiyatli emas, lekin kelajakda yuzaga kelishi mumkin bo’lgan muammolarni ko’rsatishi mumkin bo’lgan voqealar Windows OTda qanday hodisa sifatida qayd etiladi?
492. Axborot
493. Muvaffaqiyatsiz audit
494. ***Ogohlantirish***
495. Xatolik
496. Qaysi holatni normal va qaysi holatni normal bo’lmagan deb topish va ushbu ikki holat orasidagi farqni aniqlashga asoslanadi. Ushbu xususiyat zararli dasturiy vositalarni aniqlashning qaysi usuliga tegishli?
497. Barchasiga
498. Signaturaga asoslangan
499. O’zgarishni aniqlashga asoslangan
500. ***Anomaliyaga asoslangan***
501. Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo’lgan murojaatlarini chegaralash qaysi himoya vositasing vazifasi hisoblanadi?
502. Antivirus
503. Router
504. ***Tarmoqlararo ekran***
505. Virtual himoyalangan tarmoq
506. Tashqi ma’lumotlarni bazaga yuklashda qanday kengaytmali fayl formatidan foydalansa bo’ladi?
507. JPEG
508. PDF
509. CSV
510. DOCX
511. Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat’iy nazar muvaffaqiyatli o’rnatuvchi asos bu?
512. ***Tarmoq modeli***
513. Kompyuter tarmog’i
514. Mobil tarmoq
515. Tarmoq topologiyasi
516. WEP, WPA, WPA2 protokollari qaysi simsiz texnologiyada ishlatilgan?
517. WiMax
518. ***Wi-Fi***
519. GSM
520. Bluetooth
521. Zaxira nusxalash strategiyasi rejasi nimadan boshlanadi?
522. Mos zaxira nusxalash usulini tanlashdan
523. Zaxira nusxalash texnologiyasini tanlashdan
524. Zaxira nusxalash uchun xotira qurilmasini tanlashdan
525. ***Tashkilot missiyasi uchun zarur axborotni aniqlashdan***
526. Tashkilot axborot aktivlarini va binolaridan foydalanishni kuzatish, qaydlash va nazoratlashga yordam beruvchi xavfsizlik turi?
527. Iqtisodiy xavfsizlik
528. ***Fizik xavfsizlik***
529. Huquqiy xavfsizlik
530. Tarmoq xavfsizligi
531. Xavfsizlik siyosatlarining afzalliklari keltirilgan qatorni toping.
532. Kuchaytirilgan ma’lumot va tarmoq xavfsizligini ta’minlaydi
533. Qurilmalardan foydalanish va ma’lumotlar transferining monitoringlanishi va nazoratlanishini ta’minlaydi
534. ***Barcha javoblar to’g’ri***
535. Risklarni kamaytiradi
536. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to’plami bu?
537. Xavfsizlik doktorinasi
538. ***Xavfsizlik siyosati***
539. Xavfsizlik konsepsiyasi
540. Tashkilot nizomi
541. A5/1 oqimli shifrlash algoritmida maj(1,0,1) ga bo’lsa, qaysi registorlar siljiydi?
542. X,Y,Z
543. Y
544. ***X,Z***
545. X,Y
546. RSA algoritmida p=7, q=19 bo’lsa, N sonidan kichik va u bilan o’zaro tub bo’lgan sonlar miqdorini ko’rsating.
547. 133
548. 26
549. 72
550. ***108***
551. A5/1 oqimli shifrlash algoritmida maj(0,1,0) ga bo’lsa, qaysi registorlar siljiydi?
552. X,Y,Z
553. ***Y***
554. X,Z
555. X,Y
556. Ochiq kalitli shifrlash algoritmida ma’lumotni shifrlab yuborish qaysi kalit yordamida amalga oshiriladi?
557. Qabul qiluvchining shaxsiy kaliti
558. Qabul qiluvchining ochiq kaliti
559. Yuboruvchining shaxsiy kaliti
560. Yuboruvchining ochiq kaliti
561. Yong’inga qarshi tizimlarni aktiv chora turiga quyidagilardan qaysilari kiradi.
562. Yong’inga aloqador tizimlarni to’g’ri madadlanganligi
563. ***Yong’inni aniqlash va bartaraf etish tizimi***
564. Minimal darajada yonuvchan materiallardan foydalanish
565. Yetarlicha miqdorda qo’shimcha chiqish yo’llarini mavjudligi
566. Modul arifmetikasida mod11 bo’yicha 5 soniga teskari bo’lgan sonni toping?
567. ***9***
568. 4
569. 1/11
570. 1/5
571. Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko’rish rejimini kuzatib boruvchi zararli dastur turi bu?
572. Backdoors
573. ***Adware***
574. Spyware
575. Troyan otlari
576. Kompyuter viruslarini tarqalish usullarini ko’rsating.
577. Ma’lumot saqlovchilari, internetdan yuklab olish va skaner qurilmalari orqali
578. Barcha javoblar to’g’ri
579. ***Ma’lumot saqlovchilari, internetdan yuklab olish va electron pochta orqali***
580. Printer qurilmasi, internetdan yuklab olish va electron pochta orqali
581. Riskning qaysi darajasida risk ta’sirini kamaytirish uchun profilaktika choralarini ko’rish talab etiladi?
582. ***Quyi***
583. Yuqori
584. Barcha darajalarda
585. O’rta
586. Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalaniladi?
587. Apparat
588. Dasturiy
589. Simmetrik
590. Ochiq kalitli
591. RSA algoritmida ochiq kalit e=5 n=35 ga teng bo’lsa M=2 ga teng ochiq matnni shifrlash natijasini ko’rsating?
592. 35
593. 7
594. 5
595. 32
596. Modul arifmetikasida mod5 bo’yicha 4 soniga teskari bo’lgan sonni toping?
597. 20
598. 1
599. ***4***
600. 4/5
601. A5/1 shifrlash algoritmida registrlar siljiganidan keying holat: x18=0, y21=0 va z22=1 ga teng bo’lsa, hosil bo’lgan psevdotasodifiy qiymatni ko’rsating.
602. 100
603. ***0***
604. 1
605. 10
606. Simsiz lokal tarmoq texnologiyasini ko’rsating.
607. Ethernet
608. ***Wi-Fi***
609. WiMax
610. Bluetooth
611. Parollar 6 xonali uzunlikka va har bir xonasi uchun 32 ta turli belgilar bo’lishi mumkin bo’lgan jami parollar soni nechta?
612. 6^32
613. 32!
614. ***32^6***
615. 6!
616. Har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo’shilsa ….
617. Hujum paydo bo’ladi
618. ***Risk paydo bo’ladi***
619. Aktiv paydo bo’ladi
620. Tahdid paydo bo’ladi
621. Faqat ma’lumotga nisbatan o’zgarish yuz berganda zaxiralashni amalga oshiruvchi usuli?
622. Differensial zaxiralash
623. To’liq zaxiralash
624. ***O’sib boruvchi zaxiralash***
625. Ichki zaxiralash
626. Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas.
627. Turli kirishlar turli chiqishlarni akslantirishi
628. Kolliziyaga bardoshli bo’lishi
629. Amalga oshirishdagi yuqori tezkorlik
630. ***Bir tomonlama funksiya bo’lmasligi kerak***
631. Ob’yektning eng cheklangan imtiyoz turini aniqlang.
632. Private
633. Protected
634. Static
635. Public
636. Biror mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu?
637. Virus
638. Adware
639. Mantiqiy bombalar
640. Backdoors
641. Quyidagi atamalardan qaysi biri faqat simmetrik blokli shifrlarga xos?
642. Blok uzunligi
643. Kalit uzunligi
644. Kodlash jadvali
645. Ochiq kalit
646. Axborotni qaysi xususiyatlari ochiq kalitli shifrlar yordamida ta’minlanadi?
647. Foydalanuvchanlik va konfidensiallik
648. Konfidensiallik, butunlik va foydalanuvchanlik
649. Konfidensiallik
650. Butunlik va foydalanuvchanlik
651. Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi?
652. Antivirus
653. Router
654. ***Tarmoqlararo ekran***
655. Virtual himoyalangan tarmoq
656. RSA algoritmida p=5 q=11 e=7 ga teng bo’lsa, shaxsiy kalitni hisoblang.
657. ***23***
658. 35
659. 24
660. 7
661. Himoya mexanizmini aylanib o’tib tizimga ruxsatsi kirish imkonini beruvchi zarali dastur bu?
662. Troyan otlari
663. Adware
664. Spyware
665. Backdoors
666. Legitimate code

If hour is 7 p.m:

crash\_computer()

legitimate code

Ushbu mantiqiy kod qaysi zararli dasturiy vositaga tegishli?

1. Adware
2. Mantiqiy bomba
3. Virus
4. Backdoors
5. Diskdagi barcha ma’lumotlarni ( master boot record, (MBR) bilan) yoki MBRsiz shifrlashni amalga oshiradi. Gap qaysi shifrlash usuli haqida bormoqda?
6. Apparat shifrlash
7. Dasturiy shifrlash
8. Faylni shifrlash
9. Diskni shifrlash
10. “Single-pair shortest path problem” ushbu atama nimani anglatadi?
11. Ikkita tugun orasidagi eng qisqa masofani aniqlash masalasi
12. Berilgan tugundan barcha tugunlarga bo’lgan qisqa yo’llarni aniqlash masalasi
13. Berilgan punktga yetib borishning qisqaroq yo’lini aniqlash masalasi
14. 3 ta tugun orasidagi eng qisqa masofani aniqlash masalasi
15. Tarmoqdagi kompyuterlarga kabel orqali ulangan markaziy xabdan (tugun) iborat topologiya nima?
16. Shina
17. Daraxt
18. Yulduz
19. Halqa
20. Paketlarni snifferlash, portlarni skanerlash, ping buyru’gini yuborish qanday hujum turiga misol bo’ladi?
21. Zararli hujumlar
22. ***Razvedka hujumlari***
23. Xizmatdan voz kechishga undash hujumlari
24. Kirish hujumlari
25. Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi shifrlar bu –
26. Ochiq kalitli shifrlar
27. Xesh funksiyalar
28. Bir xil kalitli shifrlar
29. ***Simmetrik shifrlar***
30. Har bir obyekt uchun foydalanish ruxsatini belgilash o’rniga, rol uchun obyektlardan foydalanish ruxsatini ko’rsatish amalga oshiriladi. Gap qaysi foydalanishni boshqarish usuli haqida bormoqda?
31. MAC
32. ABAC
33. ***RBAC***
34. DAC
35. Biba modelida axborotni qaysi xususiyatini ta’minlashni maqsad qiladi?
36. Konfidensiallik
37. Butunlik
38. Foydalanuvchanlik
39. Maxfiylik
40. 2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo’yicha qo’shing?
41. 11111
42. 01100
43. 10000
44. 00001
45. Quyidagi muammolardan qaysi biri simmetrik kriptotizimlarga xos.
46. Foydalanuvchilar tomonidan maqbul ko’rilmasligi
47. Kalitlarni esda saqlash murakkabligi
48. ***Kalitni taqsimlash zaruriyati***
49. Shifrlash jarayonining ko’p vaqt olishi
50. Ma’lumotni yo’qotish yoki funksionallikni yo’qotish kabi muhim muammoni ko’rsatadigan voqealar windows OT da qanday hodisa sifatida qayd etiladi?
51. ***Xatolik***
52. Ogohlantirish
53. Muvaffaqiyatsiz audit
54. Axborot
55. Mijozlar, foydalanuvchilar va tashkilotlarda mavjud bo’lgan biror xizmatni cheklashga urinuvchi hujum bu?
56. Spufing hujumi
57. Razvedka hujumi
58. Kirish hujumi
59. ***Xizmatlardan voz kechishga undash hujumi***
60. Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko’rsating.
61. ***Ochiq kalitli shifrlar***
62. Simmetrik shifrlar
63. Oqimli shifrlar
64. Blokli shifrlar
65. Jumlani to’ldiring. Simli va simsiz tarmoqlar orasidagi asosiy farq …
66. Tarmoq chetki nuqtalari orasidagi xududning kengligi
67. Himoyani amalga oshirish imkoniyati yo’qligi
68. Himoya vositalarining chegaralanganligi
69. ***Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlanmaydigan xudud mavjudligi***
70. ERI da rad etish jarayoni - …
71. Foydalanuvchi (B) qabul qilib olingan ma’lumotni o’zgartirib, shu o’zgartirilgan ma’lumotni foydalanuvchi (A) yubordi deb ta’kidlaydi
72. (A) va (B) foydalanuvchilarning o’zaro aloqa tarmog’iga uchinchi bir (V) foydalanuvchi noqonuniy tarzda bog’lanib, ularning o’zaro uzatayotgan ma’lumotlarini o’zgartirgan holda deyarli uzluksiz uzatib turadi
73. ***Foydalanuvchi (A) foydalanuvchi (B) ga haqiqatdan ham ma’lumot jo’natgan bo’lib, uzatilgan ma’lumotni rad etishi mumkin***
74. Foydalanuvchi (B) ning o’zi ma’lumot tayyorlab, bu soxta ma’lumotni foydalanuvchi (A) yubordi deb da’vo qiladi
75. Eng kam xarajatli zaxira nusxalash manzilini ko’rsating.
76. O’sib boruvchi zaxiralash
77. Bulutda zaxiralash
78. ***Ichki zaxiralash***
79. Tashqi zaxiralash
80. Jumlani to’ldiring. Ma’lumotni uzatishda kriptografik himoya …..
81. ***Foydalanuvchanlik va butunlikni ta’minlaydi***
82. Konfidensiallik va foydalanuvchanlikni ta’minlaydi
83. Konfidensiallik va butunlikni ta’minlaydi
84. Konfidensiallik ta’minlaydi
85. Bell-Lapadula modelida birinchi ob’ektning xavfsizlik darajasi L(01) ga, ikkinchi ob’ektning xavfsizlik darajasi L(02) ga va uchinchi ob’ektning xavfsizlik darajasi L(03) teng bo’lsa, u holda uchta ob’ektdan iborat bo’lgan bo’lgan to’rtinchi ob’ektning xavfsizlik darajasi nimaga teng bo’ladi? Bu yerda L(01)<L(02)<L(03)
86. ***L(03)***
87. L(02)
88. L(01)
89. Berilgan shartlar yetarli emas
90. Qaysi himoya vositasi yetkazilgan axborotning butunligini tekshiradi?
91. Router
92. ***Virtual Private Network***
93. Tarmoqlararo ekran
94. Antivirus
95. Foydalanuvchini haqiqiyligini tekshirish jarayoni bu?
96. Identifikatsiya
97. Avtorizatsiya
98. ***Autentifikatsiya***
99. Ro’yxatga olish
100. Faqat foydalanishni boshqarish usullari keltirilgan javobni ko’rsating?
101. ***DAC, MAC***
102. ABAC, RSA
103. RBAC, A5/1
104. DAC, RSA
105. Belgilangan sharoitlarda tahdidning manbalarga potensial zarar yetkazilishini kutish bu?
106. ***Risk***
107. Tahdid
108. Zaiflik
109. Hujum
110. Quyidagilardan qaysi biri tarmoq xavfsizligi muammolariga sabab bo’lmaydi?
111. Tug’ma texnologiya zaifligi
112. ***Routerlardan foydalanmaslik***
113. Tarmoqni xavfsiz bo’lmagan tarzda va zaif loyihalash
114. Qurilma yoki dasturiy vositani noto’g’ri sozlanish
115. Tarmoqning tuzilishini aniqlab, tarmoqning mantiqiy va fizik joylashuvini hisoblaydi. Gap nima haqida bormoqda?
116. Arxitektura
117. ***Topologiya***
118. Protokol
119. Model
120. Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi?
121. Ochiq kalit
122. ***Dasturiy***
123. Simmetrik
124. Apparat
125. Tarmoq sathidagi VPN qaysi protokol asosida quriladi?
126. L2F
127. PPTP
128. TLS
129. ***IPSec***
130. Qanday tahdidlar passiv hisoblanadi?
131. Axborot xavfsizligini buzmaydigan tahdidlar
132. Amalga oshishida axborot strukturasi va mazmunida hech narsani o’zgartirmaydigan tahdidlar
133. Texnik vositalar bilan bog’liq bo’lgan tahdidlar
134. Hech qachon amalga oshirilmaydigan tahdidlar
135. Jumlani to’ldiring. Hujumchi kabi fikrlash …. Kerak.
136. ***Ma’lumot, axborot va tizimdan foydalanish uchun***
137. Ma’lumotni aniq va ishonchli ekanligini bilish uchun
138. Kafolatlangan amallarni ta’minlash uchun
139. Axborot xavfsizligida zaiflik bu?
140. Tizim yoki tshkilotga zarar yetkazishi mumkin bo’lgan istalmagan hodisa
141. Noaniqlikning maqsadlarga ta’siri
142. Tashkilot uchun qadrli bo’lgan ixtiyoriy narsa
143. ***Tahdidga sabab bo’luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson***
144. Jumlani to’ldiring. Axborot xavfsizligiga bo’ladigan … tahdidlari maqsadli (atayin) tahdidlar deb ataladi.
145. ***Foydalanuvchilar va xizmat ko’rsatuvchi hodimlarning hatoliklari***
146. Tabiiy ofat va avariya
147. Texnik vositalarning buzilishi va ishlamasligi
148. Strukturalarni ruxsatsiz modifikatsiyalash
149. ….. – ushbu zaxiralash usuli tizim ishlamay turganda yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi. Ushbu usul zaxiralashning xavfsiz usuli hisoblanib, ma’lumotni nusxalash xavfidan himoyalaydi.
150. Issiq zaxiralash
151. ***Sovuq zaxiralash***
152. Iliq zaxiralash
153. Ichki zaxiralash
154. OSI modelining quyi sathi bu?
155. ***Fizik sath***
156. Transport sathi
157. Kanal sathi
158. Tarmoq sathi
159. Bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi bu?
160. Tarmoq topologiyasi
161. Kompyuter topologiyasi
162. Tarmoq arxitekturasi
163. ***Kompyuter tarmog’i***
164. Hajmi bo’yicha eng kichik hisoblangan tarmoq turi bu –
165. CAN
166. ***PAN***
167. MAN
168. LAN
169. Tizimning turli resurslarga foydalanishni cheklash uchun foydalaniluvchi qoidalar to’plami haqidagi barcha narsalar bu?
170. ***Avtorizatsiya***
171. Autentifikatsiya
172. Identifikatsiya
173. Ruxsatlarni nazoratlash
174. Bir xil baroshlika ega bo’lganida quyidagi algoritmlardan qaysi birida kalit uzunligi eng kata bo’ladi?
175. DES
176. ***AES***
177. A5/1
178. RSA
179. 12 soni bilan o’zaro tub bo’lgan sonlarni ko’rsating.
180. 14, 26
181. 144, 4
182. 12 dan tashqari barcha sonlar
183. ***11, 13***
184. Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?
185. Barcha javoblar to’g’ri
186. Boshqa kompyuterda yozib olingan ma’lumotlarni o’qishdan oldin har bir saqlagichni antivirus tekshiruvidan o’tkazish
187. Kompyuterni zamonaviy antivirus darturiy vositasi bilan ta’minlash va uni doimiy yangilab boorish
188. Faqat litsenziyali dasturiy ta’minotdan foydalanish
189. Kirish hujumlari bu?
190. Foydalanuvchilarga va tashkilotlarda mavjud bo’lgan biror xizmatni cheklashga urinadi
191. Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to’plashni maqsad qiladi
192. Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi
193. Tarmoq haqida axborotni to’plash hujumchilarga mavjud
194. A5/1 algoritmidagi Z registor uzunligi nechiga teng?
195. 23
196. 21
197. 22
198. 19
199. Ochiq tarmoq yordamida himoyalangan tarmoqni qurish imkoniyatiga ega himoya vositasi bu?
200. Antivirus
201. Tarmoqlararo ekran
202. ***Virtual Private Network***
203. Router
204. Diskni shifrlash usuliga xos bo’lgan xususiyatlarni belgilang.
205. Faqat kriptografik kalitlar xotirada saqlanib, shifrlangan fayllar ochiq holatda saqlanadi
206. Asosiy fayl tizimining ustida joylashgan kriotografik fayl tizimidan foydalanish (masalan, ZSF, EncFS)
207. ***Deyarli barcha narsa, almashtirish maydoni (swap space), vaqtinchalik fayllar shifrlanadi***
208. Jumlani to’ldiring. Autentifikatsiya tizimlari asoslanishiga ko’ra …. turga bo’linadi.
209. 3
210. 5
211. 4
212. 2
213. Ikki kalitli kriptotizim bu –
214. MAC tizimlari
215. Simmetrik kriptotizim
216. ***Ochiq kalitli kriptotizim***
217. Xesh funksiyalar
218. Kriptologiya so’ziga berilgan to’g’ri tavsifni toping?
219. Maxfiy shifrlarni buzish fani va san’ati
220. Maxfiy shifrlarni yaratish fani va san’ati
221. ***Maxfiy shifrlarni yaratish, buzish fani va san’ati***
222. Axborotni himoyalash fani va san’ati
223. ….. axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to’plami.
224. ***Alifbo***
225. Kodlash
226. Shifrmatn
227. Ochiq matn
228. Parollar 10 xonali uzunlikka va har bir xonasi uchun 14ta turli belgilar bo’lishi mumkin bo’lgan jami parollar soni nechta?
229. 10^14
230. ***14^10***
231. 140
232. 24
233. Modul arifmetikasida mod9 bo’yicha 7 soniga teskari bo’lgan sonni toping?
234. 7/9
235. ***4***
236. 63
237. 2
238. Paket filteri turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi?
239. Ilova sathi parametrlari asosida
240. Taqdimot sathi parametrlari asosida
241. ***Tarmoq sathi parametrlari asosida***
242. Kanal sathi parametrlari asosida
243. Kriptotizimning to’liq xavfsiz bo’lishi Kerxgovs prinsipiga ko’ra qaysi kattalikning nomalum bo’lishiga asoslanadi?
244. Algoritm
245. ***Kalit***
246. Protokol
247. Shifrmatn
248. RSA algoritmida p=3, q=11 bo’lsa, N sonidan kichik va u bilan o’zaro tub bo’lgan sonlar miqdorini ko’rsating.
249. 43
250. ***20***
251. 11
252. 13
253. A5/1 algoritmidagi X registor uzunligi nechiga teng?
254. 23
255. ***19***
256. 18
257. 22
258. Qaysi himoya vositasi tomonlarni autentifikatsiyalash imkoniyatini beradi?
259. ***Virtual private network***
260. Tarmoqlararo ekran
261. Router
262. Antivirus
263. Qaysi funksiya matnli fayllar bilan ishlashda mavjud put (joylashish) pozitsiyasini ifodalaydigan streampos turdagi qiymatni qaytaradi?
264. Seekg()
265. Seekp()
266. Tellg()
267. ***Tellp()***
268. Foydalanuvchi yoki subyektni haqiqiyligini tekshirish jarayoni bu?
269. ***Autentifikatsiya***
270. Ruxsatlarni nazoratlash
271. Avtorizatsiya
272. Identifikatsiya
273. Foydalanuvchi parollari bazada qanday ko’rinishda saqlanadi?
274. Bazada saqlanmaydi
275. ***Xeshlangan ko’rinishda***
276. Shifrlangan ko’rinishda
277. Ochiq holatda
278. Qaysi bilim sohasi tashkil etuvchilar o’rtasidagi aloqani himoyalashga e’tibor qaratib, o’zida fizik va mantiqiy ulanishni birlashtiradi?
279. Dasturiy ta’minotlar xavfsizligi
280. Ma’lumotlar xavfsizligi
281. ***Aloqa xavfsizligi***
282. Tashkil etuvchilar xavfsizligi
283. Ruxsatsiz foydalanish, qo’pol kuch hujumi, imtiyozni orttirish, o’rtaga turgan odam hujumi, kabilar qaysi tarmoq xavfsizligiga kiritilgan hujumlar oilasiga tegishli?
284. Razvedka hujumlari
285. Zararli hujumlar
286. Xizmatdan voz kechishga undash hujumlari
287. ***Kirish hujumlari***
288. Axborot xavfsizligida tahdid bu?
289. Noaniqlikning maqsadlarga ta’siri
290. Tashkilot uchun qadrli bo’lgan ixtiyoriy narsa
291. ***Aktivga zarar yetkazishi mumkin bo’lgan istalmagan hodisa***
292. U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz
293. Xavfsizlik bo’shlig’i bo’lib, turli foydalanuvchilarni autentifikatsiyalash usullarini aylanib o’tib hujumchiga tizimga kirish imkoniyatini taqdim etadi. Gap nima haqida bormoqda?
294. ***Zaiflik***
295. Aktiv
296. Tahdid
297. Hujum
298. Yaxlitlikni ta’minlash bu-?
299. Ruxsatsiz bajarishdan himoyalash
300. ***Ruxsatsiz yozishdan himoyalash***
301. Ruxsatsiz o’qishdan himoyalash
302. Ruxsat etilgan amallarni bajarish
303. Plastik kartadan to’lovni amalga oshirishda mavjud autentifikatsiya usuli qaysi sinfga tegishli?
304. Bir faktorli autentifikatsiya
305. Ikki faktorli autentifikatsiya
306. Tokenga asoslangan autentifikatsiya
307. Biometrik autentifikatsiya
308. RAID 0 texnologiyasining vazifasi –
309. Diskni navbatlanishi va xatolikni nazoratlash
310. ***Diskni navbatlanishi***
311. Bloklarni navbatlash va akslantirish
312. Diskni akslantirish
313. Razvedka hujumlari bu?
314. Tizimni fizik buzishni maqsad qiladi
315. Foydalanuvchilarga va tashkilotlarga mavjud bo’lgan biror xizmatni cheklashga urinadi
316. Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi
317. ***Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to’plashni maqsad qiladi***
318. Qaysi xususiyatlar RAID texnologiyasiga xos emas?
319. Disklarni “qaynoq almashtirish” mumkin
320. Xatoliklarni nazoratlash mumkin
321. ***Shaxsiy kompyuterda foydalanish mumkin***
322. Serverlarda foydalanish mumkin
323. Axborotni mavjudligini yashirish bilan shug’ullanuvchi fan sohasi bu –
324. Kodlash
325. ***Steganografiya***
326. Kriptotahlil
327. Kriptografiya
328. Internetdagi firibgarlikning bir turi bo’lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo’lish. Gap qaysi ijtimoiy injineriya yo’nalishi haqida ketmoqda?
329. Barcha javoblar to’g’ri
330. ***Phishing***
331. Protexting
332. Spoofing
333. C=P XOR K – bir martali bloknotda shifrlash funksiyasi bo’lsa, unga mos deshifrlash funksiyasini ko’rsating? Bu yerda, P- ochiq kalit, K-kalit, C-shifrmatn
334. P = C AND K
335. P = C OR K
336. ***P = C XOR K***
337. P = C – K
338. Biror narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilari tushuniladi?
339. Token, mashinaning kaliti
340. Yuz tasviri, barmoq izi
341. Biometrik parametrlar
342. ***PIN, Parol***
343. Qaysi biometrik parameter eng yuqori universallik xususiyatiga ega?
344. Yuz tasviri
345. ***Barmoq izi***
346. Qo’l shakli
347. Ko’z qorachig’i
348. Foydalanuvchi shaxsiy xabarlarni alohida shifrlashni unutgan vaqtlarda juda qo’l keladi. Gap qaysi shifrlash usuli xususida bormoqda?
349. Apparat shifrlash
350. Faylni shifrlash
351. Dasturiy shifrlash
352. ***Diskni shifrlash***
353. Faktorlash muammosi asosida yaratilgan assimetrik shifrlash usuli.
354. El-Gamal
355. Elliptik egri chiziqga asoslangan shifrlash
356. ***RSA***
357. Diffi-Xelman
358. 64 ta belgidan iborat Sezar shifrlash usulida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin?
359. 32
360. 63!
361. 32^2
362. ***63***
363. “Yelka orqali qarash” hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan?
364. Biometrik autentifikatsiya
365. Tokenga asoslangan autentifikatsiya
366. Ko’z qorachig’iga asoslangan autentifikatsiya
367. ***Parolga asoslangan autentifikatsiya***
368. Odatda mavjud bo’lgan IP – paket to’liq shifrlanib, unga yangi IP sarlavha beriladi. Ushbu amal qaysi himoya vositasida amalga oshiriladi?
369. Antivirus vositasi
370. ***Virtual xususiy tarmoq***
371. Diskni shifrlash vositasi
372. Tarmoqlararo ekran
373. Quyidagi ta’rif windows OTdagi qaysi hodisani tavsiflaydi? Ma’lumotni yo’qotish yoki funksionallikni yo’qotish kabi muhim muammoni ko’rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, ……… hodisasi qayd etiladi.
374. Axborot
375. Muvaffaqiyatli audit
376. ***Xatolik***
377. Ogohlantirish
378. Elektron ma’lumotlarni yo’q qilishda maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o’zgaririladigan usul bu ….
379. Magnitsizlantirish
380. ***Shredirlash***
381. Yanchish
382. Formatlash
383. Virus aniq bo’lganda va xususiyatlari aniq ajratilgan holatda eng katta samaradorlika ega zararli dasturni aniqlash usulini ko’rsating?
384. Anomaliyaga asoslangan usul
385. ***Signaturaga asoslangan usul***
386. Barcha javoblar to’g’ri
387. O’zgarishga asoslangan usul
388. O’zini yaxshi va foydali dasturiy vosita sifatida ko’rsatuvchi zararli dastur turi bu?
389. Backdoors
390. ***Troyan otlari***
391. Adware
392. Spyware
393. Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ….. amalga oshiriladi.
394. Yashirish
395. Kodlash
396. ***Deshifrlash***
397. Shifrlash
398. Jumlani to’ldiring. Tizimli fikrlash …. uchun kerak.
399. Ma’lumot, axborot va tizimdan foydalanish
400. ***Kafolatlangan amallarni ta’minlash***
401. Ma’lumotni aniq va ishonchli ekanligini bilish
402. Bo’lishi mumkin bo’lgan xavfni oldini olish
403. Ma’lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi?
404. Zarur axborotni tanlashdan
405. Mos RAID sathini tanlashdan
406. Mos zaxira nusxalash vositasini tanlashdan
407. Mos zaxira nusxalash usulini tanlashdan
408. Operatsion tizimlarda keng qo’llaniluvchi foydalanishni boshqarish usuli bu?
409. ***DAC***
410. MAC
411. RBAC
412. ABAC
413. TCP/IP modelidagi ilova sathi OSI modelidagi qaysi sathlarga mos keladi?
414. ***Ilova, taqdimot va seans***
415. Ilova
416. Ilova va taqdimot
417. Seans va taqdimot
418. Yaratilishi uchun faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmi nomini ko’rsating?
419. DES
420. El-Gamal
421. A5/1
422. ***RSA***
423. Shaxsiy simsiz tarmoqlar qo’llanilish sohasini belgilang.
424. ***Tashqi qurilmalar kabellaring o’rnida***
425. Binolar va korxonalar va internet orasida belgilangan simsiz bog’lanish
426. Butun dunyo bo’yicha internetdan foydalanishda
427. Simli tarmoqlarni mobil kengaytirish
428. Agar ob’ektning xavfsizlik darajasi sub’ektning xavfsizlik darajasidan kichik yoki teng bo’lsa, u holda o’qish uchun ruxsat beriladi. Ushbu qoida qaysi foydalanishni boshqarish usuliga tegishli.
429. ABAC
430. ***MAC***
431. RMAC
432. DAC
433. Qaysi bilim sohasi foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi?
434. Tashkil etuvchilar xavfsizligi
435. Ma’lumotlar xavfsizligi
436. ***Dasturiy ta’minotlar xavfsizligi***
437. Aloqa xafsizligi
438. RSA algoritmida p=5 q=13 e=7 ga teng bo’lsa, shaxsiy kalitni hisoblang?
439. ***7***
440. 65
441. 35
442. 13
443. DNS serverlari tarmoqda qanday vazifani amalga oshiradi?
444. Tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq uchun chiqish nuqtasi vazifasini bajaradi
445. Internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlash funksiyasini amalga oshiradi
446. Ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq uchun kiruvchi nuqta vazifasini bajaradi
447. ***Xost nomlari va internet nomlarini IP manzillarga o’zgartirish va teskarisini amalga oshiradi***
448. VPNning texnik amalga oshirilishiga ko’ra turlari keltirilgan qatorni toping.
449. Kanal sathidagi VPN; tarmoq sathidagi VPN; seans sathidagi VPN
450. ***Dasturiy ko’rinishdagi VPN; maxsus shifrlash protsessoriga ega apparat vosita ko’rinishidagi VPN***
451. Marshuritizator ko’rinishidagi VPN; tarmoqlararo ko’rinishidagi VPN
452. Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN
453. Quyidagilardan qaysilari tarmoq topologiyalari hisoblanadi?
454. ***Halqa, yulduz, shina, daraxt***
455. UDP, TCP/IP, FTP
456. SMTP, HTTP, UDP
457. OSI, TCP/IP
458. Jumlani to’ldiring. Parol kalitdan ….. farq qiladi.
459. Uzunligi bilan
460. Tasodifiylik darajasi bilan
461. Belgilari bilan
462. Samaradorligi bilan
463. Portlarni va operatsion tizimni skanerlash razvedka hujumlarining qaysi turida amalga oshiriladi?
464. Passiv
465. Lug’atga asoslangan
466. DNS izi
467. ***Aktiv***