**“Kiberxavfsizlik asoslari” fanidan**

**TESTLAR**

| ?Konfidensiallikni ta’minlash bu - |
| --- |
| +ruxsatsiz o‘qishdan himoyalash. |
| -ruxsatsiz yozishdan himoyalash. |
| -ruxsatsiz bajarishdan himoyalash. |
| -ruxsat etilgan amallarni bajarish. |

| ?Foydalanuvchanlikni ta’minlash bu - |
| --- |
| +ruxsatsiz bajarishdan himoyalash. |
| -ruxsatsiz yozishdan himoyalash. |
| -ruxsatsiz o‘qishdan himoyalash. |
| -ruxsat etilgan amallarni bajarish. |

| ?Yaxlitlikni ta’minlash bu - |
| --- |
| +ruxsatsiz yozishdan himoyalash. |
| -ruxsatsiz o‘qishdan himoyalash. |
| -ruxsatsiz bajarishdan himoyalash. |
| -ruxsat etilgan amallarni bajarish. |

| ?Jumlani to‘ldiring. Hujumchi kabi fikrlash ... kerak |
| --- |
| +bo‘lishi mumkin bo‘lgan xavfni oldini olish uchun |
| -kafolatlangan amallarni ta’minlash uchun |
| -ma’lumot, axborot va tizimdan foydalanish uchun |
| -ma’lumotni aniq va ishonchli ekanligini bilish uchun |

| ?Jumlani to‘ldiring. Tizimli fikrlash ... uchun kerak |
| --- |
| +kafolatlangan amallarni ta’minlash |
| -bo‘lishi mumkin bo‘lgan xavfni oldini olish |
| -ma’lumot, axborot va tizimdan foydalanish |
| -ma’lumotni aniq va ishonchli ekanligini bilish |

| ?Axborot xavfsizligida risk bu |
| --- |
| +Manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta’sirida tahdid qilish ehtimoli. |
| -U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz. |
| -Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa. |
| -Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |

| ?Axborot xavfsizligida tahdid bu |
| --- |
| +Aktivga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
| -Noaniqlikning maqsadlarga ta’siri. |
| -U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz. |
| -Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa. |

| ?Axborot xavfsizligida aktiv bu |
| --- |
| +Tashkilot yoki foydalanuvchi uchun qadrli bo‘lgan ixtiyoriy narsa. |
| -Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
| -Noaniqlikning maqsadlarga ta’siri. |
| -U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz. |

| ?Axborot xavfsizligida zaiflik bu |
| --- |
| +Tahdidga sabab bo‘luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson. |
| -Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa. |
| -Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |
| -Noaniqlikning maqsadlarga ta’siri. |

| ?Axborot xavfsizligida boshqarish vositasi bu |
| --- |
| +Natijasi zaiflik yoki tahdidga ta’sir qiluvchi riskni o‘zgartiradigan harakatlar. |
| -Bir yoki bir nechta tahdidga sabab bo‘luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik. |
| -Tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa. |
| -Tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. |

| ?Har qanday vaziyatda biror bir hodisani yuzaga kelish ehtimoli qo‘shilsa .... |
| --- |
| +risk paydo bo‘ladi. |
| -hujum paydo bo‘ladi. |
| -tahdid paydo bo‘ladi. |
| -aktiv paydo bo‘ladi. |

| ?Jumlani to‘ldiring. Denial of service (DOS) hujumi axborotni .... xususiyatini buzushga qaratilgan? |
| --- |
| +foydalanuvchanlik |
| -butunlik |
| -konfidensiallik |
| -ishonchlilik |

| ?Jumlani to‘ldiring. ... sohasi tashkil etuvchilar xavfsizligi, aloqa xavfsizligi va dasturiy ta’minotlar xavfsizligidan iborat? |
| --- |
| +Tizim xavfsizligi |
| -Ma’lumotlar xavfsizligi |
| -Inson xavfsizligi |
| -Tashkilot xavfsizligi |

| ?Kriptologiya so‘ziga berilgan to‘g‘ri tavsifni toping? |
| --- |
| +Maxfiy shifrlarni yaratish va buzish fani va sanati. |
| -Maxfiy shifrlarni yaratish fani va sanati. |
| -Maxfiy shifrlarni buzish fani va sanati. |
| -Axborotni himoyalash fani va sanati. |

| ?.... kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi? |
| --- |
| +Kriptografik kalit |
| -Ochiq matn |
| -Alifbo |
| -Algoritm |

| ?Kriptografiya so‘ziga berilgan to‘g‘ri tavsifni toping? |
| --- |
| +Maxfiy shifrlarni yaratish fani va sanati. |
| -Maxfiy shifrlarni yaratish va buzish fani va sanati. |
| -Maxfiy shifrlarni buzish fani va sanati. |
| -Axborotni himoyalash fani va sanati. |

| ?Kriptotahlil so‘ziga berilgan to‘g‘ri tavsifni toping? |
| --- |
| +Maxfiy shifrlarni buzish fani va sanati. |
| -Maxfiy shifrlarni yaratish fani va sanati. |
| -Maxfiy shifrlarni yaratish va buzish fani va sanati. |
| -Axborotni himoyalash fani va sanati. |

| ?..... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to‘plami. |
| --- |
| +Alifbo |
| -Ochiq matn |
| -Shifrmatn |
| -Kodlash |

| ?Ma’lumot shifrlansa, natijasi .... bo‘ladi. |
| --- |
| +shifrmatn |
| -ochiq matn |
| -nomalum |
| -kod |

| ?Deshifrlash uchun kalit va ..... kerak bo‘ladi. |
| --- |
| +shifrmatn |
| -ochiq matn |
| -kodlash |
| -alifbo |

| ?Ma’lumotni shifrlash va deshifrlashda yagona kalitdan foydalanuvchi tizim bu - |
| --- |
| +simmetrik kriptotizim. |
| -ochiq kalitli kriptotizim. |
| -asimetrik kriptotizim. |
| -xesh funksiyalar. |

| ?Ikki kalitli kriptotizim bu - |
| --- |
| +ochiq kalitli kriptotizim. |
| -simmetrik kriptotizim. |
| -xesh funksiyalar. |
| -MAC tizimlari. |

| ?Axborotni mavjudligini yashirish bilan shug‘ullanuvchi fan sohasi bu - |
| --- |
| +steganografiya. |
| -kriptografiya. |
| -kodlash. |
| -kriptotahlil. |

| ?Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ..... amalga oshiriladi. |
| --- |
| +kodlash |
| -shifrlash |
| -yashirish |
| -deshifrlash |

| ?Jumlani to‘ldiring. Ma’lumotni konfidensialligini ta’minlash uchun ..... zarur. |
| --- |
| +shifrlash |
| -kodlash |
| -dekodlash |
| -deshifrlash |

| ?Ma’lumotni mavjudligini yashirishda ..... |
| --- |
| +steganografik algoritmdan foydalaniladi. |
| -kriptografik algoritmdan foydalaniladi. |
| -kodlash algoritmidan foydalaniladi. |
| -kriptotahlil algoritmidan foydalaniladi. |

| ?Xesh funksiyalar - .... funksiya. |
| --- |
| +kalitsiz kriptografik |
| -bir kalitli kriptografik |
| -ikki kalitli kriptografik |
| -ko‘p kalitli kriptografik |

| ?Jumlani to‘ldiring. Ma’lumotni uzatishda kriptografik himoya ..... |
| --- |
| +konfidensiallik va butunlikni ta’minlaydi. |
| -konfidensiallik va foydalanuvchanlikni ta’minlaydi. |
| -foydalanuvchanlik va butunlikni ta’minlaydi. |
| -konfidensiallik ta’minlaydi. |

| ?Jumlani to‘ldiring. ... kompyuter davriga tegishli shifrlarga misol bo‘la oladi. |
| --- |
| +DES, AES shifri |
| -Sezar shifri |
| -Kodlar kitobi |
| -Enigma shifri |

| ?.... kriptografik shifrlash algoritmlari blokli va oqimli turlarga ajratiladi. |
| --- |
| +Simmetrik |
| -Ochiq kalitli |
| -Asimmetrik |
| -Klassik davr |

| ?Jumlani to‘ldiring. .... shifrlar tasodifiy ketma-ketliklarni generatsiyalashga asoslanadi. |
| --- |
| +Oqimli |
| -Blokli |
| -Ochiq kalitli |
| -Asimetrik |

| ?Ochiq matn qismlarini takroriy shifrlovchi algoritmlar bu - |
| --- |
| +blokli shifrlar |
| -oqimli shifrlash |
| -ochiq kalitli shifrlar |
| -asimmetrik shifrlar |

| ?A5/1 shifri bu - |
| --- |
| +oqimli shifr. |
| -blokli shifr. |
| -ochiq kalitli shifr. |
| -asimmetrik shifr |

| ?Quyidagi muammolardan qaysi biri simmetrik kriptotizimlarga xos. |
| --- |
| +Kalitni taqsimlash zaruriyati. |
| -Shifrlash jarayonining ko‘p vaqt olishi. |
| -Kalitlarni esda saqlash murakkabligi. |
| -Foydalanuvchilar tomonidan maqbul ko‘rilmasligi. |

| ?Quyidagi atamalardan qaysi biri faqat simmetrik blokli shifrlarga xos? |
| --- |
| +Blok uzunligi. |
| -Kalit uzunligi. |
| -Ochiq kalit. |
| -Kodlash jadvali. |

| ?Jumlani to‘ldiring. Sezar shifri .... akslantirishga asoslangan. |
| --- |
| +o‘rniga qo‘yish |
| -o‘rin almashtirish |
| -ochiq kalitli |
| -kombinatsion |

| ?Kriptotizimning to‘liq xavfsiz bo‘lishi Kerxgofs prinsipiga ko‘ra qaysi kattalikning nomalum bo‘lishiga asoslanadi? |
| --- |
| +Kalit. |
| -Algoritm. |
| -Shifrmatn. |
| -Protokol. |

| ?Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi shifrlar bu - |
| --- |
| +ochiq kalitli shifrlar. |
| -simmetrik shifrlar. |
| -bir kalitli shifrlar |
| -xesh funksiyalar. |

| ?Hujumchi kabi fikrlash bu, |
| --- |
| +Kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarni o‘zaro ta’sirini hisobga oladigan fikrlash jarayoni. |
| -Tizim ma’lumoti va axborotiga faqat vakolatga ega sub’ektlar foydalanishi mumkinligini ta’minlovchi qoidalar. Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o‘qilishini” ta’minlaydi. |
| -Bo‘lishi mumkin bo‘lgan xavfni oldini olish uchun qonuniy foydalanuvchini hujumchi kabi fikrlash jarayoni. |
| -Ma’lumot, axborot va tizimdan foydalanishning mumkinligi. Ya’ni, ruxsat etilmagan “bajarish” dan himoyalash. |

| ?Axborotni qaysi xususiyatlari simmetrik shifrlar yordamida ta’minlanadi. |
| --- |
| +Konfidensiallik va butunlik. |
| -Konfidensiallik. |
| -Butunlik va foydalanuvchanlik. |
| -Foydalanuvchanlik va konfidensiallik. |

| ?Axborotni qaysi xususiyatlari ochiq kalitli shifrlar yordamida ta’minlanadi. |
| --- |
| +Konfidensiallik. |
| -Konfidensiallik, butunlik va foydalanuvchanlik. |
| -Butunlik va foydalanuvchanlik. |
| -Foydalanuvchanlik va konfidensiallik. |

| ?Quyidagilardan qaysi biri rad etishdan himoyani ta’minlaydi. |
| --- |
| +Elektron raqamli imzo tizimi. |
| -MAC tizimlari. |
| -Simmetrik shifrlash tizimlari. |
| -Xesh funksiyalar. |

| ?Qaysi ochiq kalitli algoritm katta sonni faktorlash muammosiga asoslanadi? |
| --- |
| +RSA algoritmi. |
| -El-Gamal algoritmi. |
| -DES. |
| -TEA. |

| ?Rad etishdan himoyalashda ochiq kalitli kriptotizimlarning qaysi xususiyati muhim hisoblanadi. |
| --- |
| +Ikkita kalitdan foydalanilgani. |
| -Matematik muammoga asoslanilgani. |
| -Ochiq kalitni saqlash zaruriyati mavjud emasligi. |
| -Shaxsiy kalitni saqlash zarurligi. |

| ?Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas. |
| --- |
| +Bir tomonlama funksiya bo‘lmasligi kerak. |
| -Amalga oshirishdagi yuqori tezkorlik. |
| -Turli kirishlar turli chiqishlarni akslantirishi. |
| -Kolliziyaga bardoshli bo‘lishi. |

| ?Quyidagi xususiyatlardan qaysi biri elektron raqamli imzo tomonidan ta’minlanadi? |
| --- |
| +Axborot butunligini va rad etishdan himoyalash. |
| -Axborot konfidensialligini va rad etishdan himoyalash. |
| -Axborot konfidensialligi. |
| -Axborot butunligi. |

| ?Faqat ma’lumotni butunligini ta’minlovchi kriptotizimlarni ko‘rsating. |
| --- |
| +MAC (Xabarlarni autentifikatsiya kodlari) tizimlari. |
| -Elektron raqamli imzo tizimlari. |
| -Ochiq kalitli kriptografik tizimlar. |
| -Barcha javoblar to‘g‘ri. |

| ?Foydalanuvchini tizimga tanitish jarayoni bu? |
| --- |
| +Identifikatsiya. |
| -Autentifikatsiya. |
| -Avtorizatsiya. |
| -Ro‘yxatga olish. |

| ?Foydalanuvchini haqiqiyligini tekshirish jarayoni bu? |
| --- |
| +Autentifikatsiya. |
| -Identifikatsiya. |
| -Avtorizatsiya. |
| -Ro‘yxatga olish. |

| ?Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu? |
| --- |
| +Avtorizatsiya. |
| -Autentifikatsiya. |
| -Identifikatsiya. |
| -Ro‘yxatga olish. |

| ?Parolga asoslangan autentifikatsiya usulining asosiy kamchiligini ko‘rsating? |
| --- |
| +Esda saqlash zaruriyati. |
| -Birga olib yurish zaririyati. |
| -Almashtirib bo‘lmaslik. |
| -Qalbakilashtirish mumkinligi. |

| ?Biror narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilar tushuniladi. |
| --- |
| +PIN, Parol. |
| -Token, mashinaning kaliti. |
| -Yuz tasviri, barmoq izi. |
| -Biometrik parametrlar. |

| ?Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting? |
| --- |
| +Doimo xavfsiz saqlab olib yurish zaruriyati. |
| -Doimo esada saqlash zaruriyati. |
| -Qalbakilashtirish muammosi mavjudligi. |
| -Almashtirib bo‘lmaslik. |

| ?Esda saqlashni va olib yurishni talab etmaydigan autentifikatsiya usuli bu - |
| --- |
| +biometrik autentifikatsiya. |
| -parolga asoslangan autentifikatsiya. |
| -tokenga asoslangan autentifikatsiya. |
| -ko‘p faktorli autentifikatsiya. |

| ?Qaysi biometrik parametr eng yuqori universallik xususiyatiga ega? |
| --- |
| +Yuz tasviri. |
| -Ko‘z qorachig‘i. |
| -Barmoq izi. |
| -Qo‘l shakli. |

| ?Qaysi biometrik parametr eng yuqori takrorlanmaslik xususiyatiga ega? |
| --- |
| +Ko‘z qorachig‘i. |
| -Yuz tasviri. |
| -Barmoq izi. |
| -Qo‘l shakli. |

| ?Quyidagilardan qaysi biri har ikkala tomonning haqiqiyligini tekshirish jarayonini ifodalaydi? |
| --- |
| +Ikki tomonlama autentifikatsiya. |
| -Ikki faktorli autentifikatsiya. |
| -Ko‘p faktorli autentifikatsiya. |
| -Biometrik autentifikatsiya. |

| ?Parolga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko‘rsating? |
| --- |
| +Parollar lug‘atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum. |
| -Fizik o‘g‘irlash hujumi, yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum. |
| -Parollar lug‘atidan foydalanish asosida hujum, yelka orqali qarash hujumi, qalbakilashtirish hujumi. |
| -Parollar lug‘atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararli dasturlardan foydanish asosida hujum. |

| ?Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko‘rsating? |
| --- |
| +Fizik o‘g‘irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar |
| -Parollar lug‘atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum |
| -Fizik o‘g‘irlash, yelka orqali qarash hujumi, zararli dasturlardan foydalanishga asoslangan hujumlar |
| -Parollar lug‘atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararli dasturlardan foydalanish asosida hujum |

| ?Foydalanuvchi parollari bazada qanday ko‘rinishda saqlanadi? |
| --- |
| +Xeshlangan ko‘rinishda. |
| -Shifrlangan ko‘rinishda. |
| -Ochiq holatda. |
| -Bazada saqlanmaydi. |

| ?Haqiqiy shifrlanmagan ma’lumot bu. |
| --- |
| +shifrmatn |
| -ochiq matn |
| -deshifrlash |
| -kalit |

| ?Parolni “salt” (tuz) kattaligidan foydalanib xeshlashdan (h(password, salt)) asosiy maqsad nima? |
| --- |
| +Buzg‘unchiga ortiqcha hisoblashni talab etuvchi murakkablikni yaratish. |
| -Buzg‘unchi topa olmasligi uchun yangi nomalum kiritish. |
| -Xesh qiymatni tasodifiylik darajasini oshirish. |
| -Xesh qiymatni qaytmaslik talabini oshirish. |

| ?Quyidagilardan qaysi biri tabiy tahdidga misol bo‘ladi? |
| --- |
| +Yong‘in, suv toshishi, harorat ortishi. |
| -Yong‘in, o‘g‘irlik, qisqa tutashuvlar. |
| -Suv toshishi, namlikni ortib ketishi, bosqinchilik. |
| -Bosqinchilik, terrorizm, o‘g‘irlik. |

| ?Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan? |
| --- |
| +Ma’muriy nazoratlash. |
| -Fizik nazoratlash. |
| -Texnik nazoratlash. |
| -Apparat nazoratlash. |

| ?Faqat ob’ektning egasi tomonidan foydalanishga mos bo‘lgan mantiqiy foydalanish usulini ko‘rsating? |
| --- |
| +Diskretsion foydalanishni boshqarish. |
| -Mandatli foydalanishni boshqarish. |
| -Rolga asoslangan foydalanishni boshqarish. |
| -Attributga asoslangan foydalanishni boshqarish. |

| ?Qaysi usul ob’ektlar va sub’ektlarni klassifikatsiyalashga asoslangan? |
| --- |
| +Mandatli foydalanishni boshqarish. |
| -Diskretsion foydalanishni boshqarish. |
| -Rolga asoslangan foydalanishni boshqarish. |
| -Attributga asoslangan foydalanishni boshqarish. |

| ?Biror faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami bu? |
| --- |
| +Rol. |
| -Imtiyoz. |
| -Daraja. |
| -Imkoniyat. |

| ?Qoida, siyosat, qoida va siyosatni mujassamlashtirgan algoritmlar, majburiyatlar va maslahatlar kabi tushunchalar qaysi foydalanishni boshqarish usuliga aloqador. |
| --- |
| +Attributga asoslangan foydalanishni boshqarish. |
| -Rolga asoslangan foydalanishni boshqarish. |
| -Mandatli foydalanishni boshqarish. |
| -Diskretsion foydalanishni boshqarish. |

| ?Bell-Lapadula modeli axborotni qaysi xususiyatini ta’minlashni maqsad qiladi? |
| --- |
| +Konfidensiallik. |
| -Butunlik. |
| -Foydalanuvchanlik. |
| -Ishonchlilik. |

| ?Biba modeli axborotni qaysi xususiyatini ta’minlashni maqsad qiladi? |
| --- |
| +Butunlik. |
| -Konfidensiallik. |
| -Foydalanuvchanlik. |
| -Maxfiylik. |

| ?Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi? |
| --- |
| +Apparat. |
| -Dasturiy. |
| -Simmetrik. |
| -Ochiq kalitli. |

| ?Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalanadi? |
| --- |
| +Dasturiy. |
| -Apparat. |
| -Simmetrik. |
| -Ochiq kalitli. |

| ?Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko‘rsating? |
| --- |
| +Ochiq kalitli shifrlar. |
| -Simmetrik shifrlar. |
| -Blokli shifrlar. |
| -Oqimli shifrlar. |

| ?Xesh funksiyalarda kolliziya hodisasi bu? |
| --- |
| +Ikki turli matnlarning xesh qiymatlarini bir xil bo‘lishi. |
| -Cheksiz uzunlikdagi axborotni xeshlay olishi. |
| -Tezkorlikda xeshlash imkoniyati. |
| -Turli matnlar uchun turli xesh qiymatlarni hosil bo‘lishi. |

| ?Kodlashtirish bu? |
| --- |
| mahfiy xabar mazmunini shifrlash, ya’ni ma’lumotlarni maxsus algoritm bo‘yicha o‘zgartirib, +shifrlangan matnni yaratish yo‘li bilan axborotga ruxsat etilmagan kirishga to‘siq qo‘yish usuliga aytiladi. |
| -axborotni bir tizimdan boshqa tizimga ma’lum bir belgilar yordamida belgilangan tartib bo‘yicha o‘tkazish jarayoniga aytiladi. |
| -axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi. |
| -matnni shifrlash va shifrini ochish uchun kerakli axborot. |

| ?Elektron raqamli imzo muolajalarini ko‘rsating? |
| --- |
| +Imzoni shakllantirish va imkoni tekshirish. |
| -Shifrlash va deshifrlash. |
| -Imzoni xeshlash va xesh matnni deshifrlash. |
| -Imzoni shakllartirish va xeshlash. |

| ?“Yelka orqali qarash” hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan. |
| --- |
| +Parolga asoslangan autentifikatsiya. |
| -Tokenga asoslangan autentifikatsiya. |
| -Biometrik autentifikatsiya. |
| -Ko‘z qorachig‘iga asoslangan autentifikatsiya. |

| ?Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan. |
| --- |
| +Parolga asoslangan autentifikatsiya. |
| -Tokenga asoslangan autentifikatsiya. |
| -Biometrik autentifikatsiya. |
| -Ko‘z qorachig‘iga asoslangan autentifikatsiya. |

| ?Yo‘qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon. |
| --- |
| +Parolga asoslangan autentifikatsiya. |
| -Tokenga asoslangan autentifikatsiya. |
| -Biometrik autentifikatsiya. |
| -Ko‘z qorachig‘iga asoslangan autentifikatsiya. |

| ?Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan. |
| --- |
| +Biometrik autentifikatsiya. |
| -Biror narsani bilishga asoslangan autentifikatsiya. |
| -Biror narsaga egalik qilishga asoslangan autentifikatsiya. |
| -Tokenga asoslangan autentifikatsiya |

| ?Axborotni butunligini ta’minlash usullarini ko‘rsating. |
| --- |
| +Xesh funksiyalar, MAC. |
| -Shifrlash usullari. |
| -Assimetrik shifrlash usullari, CRC tizimlari. |
| -Shifrlash usullari, CRC tizimlari. |

| ?Quyidagilardan qaysi biri to‘liq kompyuter topologiyalarini ifodalamaydi. |
| --- |
| +LAN, GAN, OSI. |
| -Yulduz, WAN, TCP/IP. |
| -Daraxt, IP, OSI. |
| -Shina, UDP, FTP. |

| ?OSI tarmoq modeli nechta sathdan iborat? |
| --- |
| +7 |
| -4 |
| -6 |
| -5 |

| ?TCP/IP tarmoq modeli nechta sathdan iborat? |
| --- |
| +4 |
| -7 |
| -6 |
| -5 |

| ?Hajmi bo‘yicha eng kichik hisoblangan tarmoq turi bu - |
| --- |
| +PAN |
| -LAN |
| -CAN |
| -MAN |

| ?Qayd etish tizimda nima deyiladi? |
| --- |
| +Ma’murlash |
| -Tasdiqlash |
| -Tekshirish |
| -Yuqotish |

| ?IP manzilni domen nomlariga yoki aksincha almashtirishni amalga oshiruvchi xizmat bu- |
| --- |
| +DNS |
| -TCP/IP |
| -OSI |
| -UDP |

| ?Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi hodisalarning potensial paydo bo‘lishi bu? |
| --- |
| +Tahdid. |
| -Zaiflik. |
| -Hujum. |
| -Aktiv. |

| ?Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat bu? |
| --- |
| +Hujum. |
| -Zaiflik. |
| -Tahdid. |
| -Zararli harakat. |

| ?Quyidagilardan qaysi biri tarmoq xavfsizligi muammolariga sabab bo‘lmaydi? |
| --- |
| +Routerlardan foydalanmaslik. |
| -Qurilma yoki dasturiy vositani noto‘g‘ri sozlanish. |
| -Tarmoqni xavfsiz bo‘lmagan tarzda va zaif loyihalash. |
| -Tug‘ma texnologiya zaifligi. |

| ?Tarmoq xavfsizligini buzulishi biznes faoliyatga qanday ta’sir qiladi? |
| --- |
| +Biznes faoliyatning buzilishi, huquqiy javobgarlikka sababchi bo‘ladi. |
| -Axborotni o‘g‘irlanishi, tarmoq qurilmalarini fizik buzilishiga olib keladi. |
| -Maxfiylikni yo‘qolishi, tarmoq qurilmalarini fizik buzilishiga olib keladi. |
| -Huquqiy javobgarlik, tarmoq qurilmalarini fizik buzilishiga olib keladi. |

| ?Razvedka hujumlari bu? |
| --- |
| +Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi. |
| -Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. |
| -Foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi. |
| -Tizimni fizik buzishni maqsad qiladi. |

| ?Kirish hujumlari bu? |
| --- |
| +Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. |
| -Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi. |
| -Foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi. |
| -Tarmoq haqida axborotni to‘plash hujumchilarga mavjud bo‘lgan potensial zaiflikni aniqlashga harakat qiladi. |

| ?Xizmatdan vos kechishga qaratilgan hujumlar bu? |
| --- |
| +Foydalanuvchilarga va tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi. |
| -Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. |
| -Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to‘plashni maqsad qiladi. |
| -Tarmoq haqida axborotni to‘plash hujumchilarga mavjud bo‘lgan potensial zaiflikni aniqlashga harakat qiladi. |

| ?Paketlarni snifferlash, portlarni skanerlash va Ping buyrug‘ini yuborish hujumlari qaysi hujumlar toifasiga kiradi? |
| --- |
| +Razvedka hujumlari. |
| -Kirish hujumlari. |
| -DOS hujumlari. |
| -Zararli dasturlar yordamida amalga oshiriladigan hujumlar. |

| ?O‘zini yaxshi va foydali dasturiy vosita sifatida ko‘rsatuvchi zararli dastur turi bu? |
| --- |
| +Troyan otlari. |
| -Adware. |
| -Spyware. |
| -Backdoors. |

| ?Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi zararli dastur turi bu? |
| --- |
| +Adware. |
| -Troyan otlari. |
| -Spyware. |
| -Backdoors. |

| ?Himoya mexanizmini aylanib o‘tib tizimga ruxsatsiz kirish imkonini beruvchi zararli dastur turi bu? |
| --- |
| +Backdoors. |
| -Adware. |
| -Troyan otlari. |
| -Spyware. |

| ?Paket filterlari turidagi tarmoqlararo ekran vositasi OSI modelining qaysi sathida ishlaydi? |
| --- |
| +Tarmoq sathida. |
| -Transport sathida. |
| -Ilova sathida. |
| -Kanal sathida. |

| ?Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi. |
| --- |
| +Tarmoqlararo ekran. |
| -Antivirus. |
| -Virtual himoyalangan tarmoq. |
| -Router. |