# TEST TOPSHIRIQLARI

№1 Fan bobi – 2; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| Kiberjinoyat quroli? |
| A. internet va eng soʻnggi raqamli texnologiyalar. |
| B. tarmoqlarning foydaluvchilari |
| C. ishchi stantsiyalar, serverlar, shaxslar |
| D. professional mutaxassislar ish faoliyati |

№2 Fan bobi – 3; Boʻlimi – 1; Qiyinchilik darajasi – 2;

|  |
| --- |
| Cyberspace internet - |
| A. bu kompyuter tarmoqlarining shartli muhitida ishlaydigan virtual  kompyuter dunyosi. |
| B. tarmoqlarda shartli muhitida ishlamaydigan virtual kompyuter dunyosi. |
| C. Serverlar va aloqa uskunalari |
| D. Aloqa kanallarida tartiblanish |

№3 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| …. - tizimlar va ularda ishlaydigan dasturiy taʻminotdagi xavfsizlik  zaifliklarini aniqlash, baholash, davolash va hisobot berish jarayonidir. |
| A. Tarmoqdagi zaifliklarni boshqarish |
| B. Tarmoqdagi zaifliklarni olib tashlash |
| C. Tarmoqdagi zaifliklarni yuq qilish |
| D. Tarmoqdagi zaifliklarbosqichlarini aniqlash |

№4 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| …. - nazoratsiz yoki kam nazorat qilinadigan hudud orqali katta boʻshliqqa  qarab, imkoniyatni taqdim etadi. |
| A. Aloqa kanallari |
| B. video monitorlar |
| C. Ishchi stantsiyalar |
| D. Serverlar va aloqa uskunalari |

№5 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tashkilotda zaifliklarni toʻgʻri boshqarishni taʻminlashning nechta bosqichi  taklif etiladi? |
| A. 5 |
| B. 4 |
| C. 3 |
| D. 2 |

№6 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tashkilotda zaifliklarni toʻgʻri boshqarishni taʻminlashning 1-bosqichi  qanday ataladi? |
| A. Boshlovchi |
| B. Takrorlanuvchi |
| C. Oʻrnatilgan |
| D. Optimallashtirish |

№7 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tashkilotda zaifliklarni toʻgʻri boshqarishni taʻminlashning 2-bosqichi  qanday ataladi? |
| A. Takrorlanuvchi |
| B. Boshlovchi |
| C. Oʻrnatilgan |
| D. Optimallashtirish |

№8 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tashkilotda zaifliklarni toʻgʻri boshqarishni taʻminlashning 3-bosqichi  qanday ataladi? |
| A. Oʻrnatilgan |
| B. Boshlovchi |
| C. Takrorlanuvchi |
| D. Optimallashtirish |

№9 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tashkilotda zaifliklarni toʻgʻri boshqarishni taʻminlashning 4-bosqichi  qanday ataladi? |
| A. Boshqariluvchi |
| B. Boshlovchi |
| C. Takrorlanuvchi |
| D. Optimallashtirish |

№10 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tashkilotda zaifliklarni toʻgʻri boshqarishni taʻminlashning 3-bosqichi  qanday ataladi? |
| A. Optimallashtirish |
| B. Boshlovchi |
| C. Takrorlanuvchi |
| D. Oʻrnatilgan |

№11 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tarmoq xavfsizligini baholashning nechta asosiy bosqichi mavjud? |
| A. 4 |
| B. 3 |
| C. 2 |
| D. 5 |

№12 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tarmoq xavfsizligini baholash jarayonining maʻlumotlarni yigʻish  bosqichida... |
| A. ….Internet Control Message Protocol (ICMP) yoki TCP protokollari  yordamida real vaqt rejimida skanerlash orqali tarmoq qurilmalarini qidirish amalga oshiriladi. |
| B. …xizmat yoki dastur ishlaydigan maxsus mashina aniqlanadi va potentsial  zaif joylar baholanadi. |
| C. …tizimga imtiyozli kirish uchun bir yoki bir nechta zaifliklardan  foydalaniladi, soʻngra ushbu kompyuterda yoki butun tarmoq yoki domenda vakolatlar kengaytiriladi. |
| D. …berilgan maʻlumotlarga boʻlgan munosabatini qabul qilish va qayd etish  bajariladi. |

№13 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tarmoq xavfsizligini baholash jarayonining bogʻlash va baholash  bosqichlarida... |
| A. …. xizmat yoki dastur ishlaydigan maxsus mashina aniqlanadi va  potentsial zaif joylar baholanadi. |
| B. … Internet Control Message Protocol (ICMP) yoki TCP protokollari yordamida real vaqt rejimida skanerlash orqali tarmoq qurilmalarini qidirish  amalga oshiriladi. |
| C. …tizimga imtiyozli kirish uchun bir yoki bir nechta zaifliklardan foydalaniladi, soʻngra ushbu kompyuterda yoki butun tarmoq yoki domenda  vakolatlar kengaytiriladi. |
| D. …berilgan maʻlumotlarga boʻlgan munosabatini qabul qilish va qayd etish  bajariladi. |

№14 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tarmoq xavfsizligini baholash jarayonining kirishish bosqichida... |
| A. …. tizimga imtiyozli kirish uchun bir yoki bir nechta zaifliklardan  foydalaniladi, soʻngra ushbu kompyuterda yoki butun tarmoq yoki domenda vakolatlar kengaytiriladi. |
| B. … Internet Control Message Protocol (ICMP) yoki TCP protokollari  yordamida real vaqt rejimida skanerlash orqali tarmoq qurilmalarini qidirish amalga oshiriladi. |
| C. … xizmat yoki dastur ishlaydigan maxsus mashina aniqlanadi va potentsial |

|  |
| --- |
| zaif joylar baholanadi. |
| D. …berilgan maʻlumotlarga boʻlgan munosabatini qabul qilish va qayd etish  bajariladi. |

№15 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Zararli kodni qidirish texnologiyalari komponentalarini belgilang. |
| A. Texnik va analitik |
| B. Passiv va faol |
| C. 1-darajali va 2-darajali |
| D. evristik va signaturali |

№16 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| .... - tahlil qilish uchun maʻlumotlarning analitik komponentini taʻminlovchi  dasturiy funktsiyalar va algoritmlar toʻplamidir. |
| A. Texnik komponent |
| B. Analitik komponent |
| C. Passiv komponent |
| D. Faol komponent |

№17 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| .... - bu uning ixtiyorida mavjud boʻlgan maʻlumotlarni tahlil qiladigan va ular  haqida bir xil qaror chiqaradigan algoritmdir. |
| A. Analitik komponent |
| B. Texnik komponent |
| C. Passiv komponent |
| D. Faol component |

№18 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| ….. - bu maʻlum operatsiyalarni avtomatik ravishda bajarish uchun  moʻljallangan dasturlar. |
| A. Botlar |
| B. Ransomware |
| C. Rootkitlar |
| D. Troyanlar |

№19 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| ... - uchinchi tomonga kompyuterga masofadan kirish va boshqarish imkonini  beradi. |

|  |
| --- |
| A. Rootkitlar |
| B. Botlar |
| C. Ransomware |
| D. Troyanlar |

№20 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| ... - kompyuteringizga zarar yetkazadi, soʻngra shaxsiy hujjatlar yoki fotosuratlar kabi nozik maʻlumotlarni shifrlaydi va ularni parolini ochish uchun  toʻlov talab qiladi. |
| A. Ransomware |
| B. Troyanlar |
| C. Botlar |
| D. Rootkitlar |

№21 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Texnogen tahdidlarning ichki manbalari berilgan qatorni belgilang. |
| A. sertifikatlanmagan va litsenziyalanmagan dasturiy taʻminot, monitoring imkoniyatlari zaif boʻlgan axborot tarmoqlari faoliyatini monitoring qilish  vositalari |
| B. ulanish kanallari, muhandislik-texnik tarmoqlar |
| C. Internet provayderlari va bulutli texnologiya provayderlari |
| D. notoʻgʻri yoki past sifatli uskunalar, muhandislik-texnik tarmoqlar |

№22 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Texnogen tahdidlarning tashqi manbalari berilgan qatorni belgilang. |
| A. Internet provayderlari va bulutli texnologiya provayderlari, ulanish  kanallari, muhandislik-texnik tarmoqlar |
| B. binolar va xodimlarni nazorat qilishning sifatsiz vositalari; |
| C. sertifikatlanmagan va litsenziyalanmagan dasturiy taʻminot, monitoring imkoniyatlari zaif boʻlgan axborot tarmoqlari faoliyatini monitoring qilish  vositalari |
| D. notoʻgʻri yoki past sifatli uskunalar, muhandislik-texnik tarmoqlar |

№23 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| SOC (Security Operations Center) tahliliy imkoniyatlarini belgilang. |
| A. Prognozlash, Aniqlash, Oldini olish, Reaksiya |
| B. dasturlar va axborot tizimlarini boshqarish |
| C. texnik jihozlardan foydalanish |

|  |
| --- |
| D. tayyor dasturiy taʻminotni yuklash, texnik jihozlardan foydalanish |

№24 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidlarni tahlil qilish uchun asosiy SOC elementi, yaʻni bilimlarni  boshqarish bu - … |
| A. SOCl mutahassislari tobora murakkablashib borayotgan hujumlarning oldini olish va ularga samarali javob berish uchun raqamli sud ekspertizasi,  zararli dasturlarni tahlil qilish |
| B. Ichki tahdidlar toʻgʻrisidagi maʻlumotlar, ommaviy axborot manbalaridan  olingan tahlillar |
| C. Anʻanaviy himoya vositalari (xavfsizlik devorlari, hujumlarni aniqlash va  oldini olish tizimlari, SIEM va boshqalar) bilan aniqlab boʻlmaydigan zararli harakatlar haqida oldindan bilib olishga imkon beradi |
| D. Toʻgʻri qurilgan hodisaga javob berish jarayoni, bu zararni cheklash va  oqibatlarini bartaraf etish xarajatlarini kamaytirish imkonini beradi |

№25 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidlarni tahlil qilish uchun asosiy SOC elementi, yaʻni yigʻilgan  materiallar asosida tahdid tahlili bu - … |
| A. Ichki tahdidlar toʻgʻrisidagi maʻlumotlar, ommaviy axborot manbalaridan  olingan tahlillar |
| B. SOCl mutahassislari tobora murakkablashib borayotgan hujumlarning oldini olish va ularga samarali javob berish uchun raqamli sud ekspertizasi,  zararli dasturlarni tahlil qilish |
| C. Anʻanaviy himoya vositalari (xavfsizlik devorlari, hujumlarni aniqlash va  oldini olish tizimlari, SIEM va boshqalar) bilan aniqlab boʻlmaydigan zararli harakatlar haqida oldindan bilib olishga imkon beradi |
| D. Toʻgʻri qurilgan hodisaga javob berish jarayoni, bu zararni cheklash va  oqibatlarini bartaraf etish xarajatlarini kamaytirish imkonini beradi |

№26 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidlarni tahlil qilish uchun asosiy SOC elementi, yaʻni tahdidlarni faol  qidirish bu - … |
| A. Anʻanaviy himoya vositalari (xavfsizlik devorlari, hujumlarni aniqlash va oldini olish tizimlari, SIEM va boshqalar) bilan aniqlab boʻlmaydigan zararli  harakatlar haqida oldindan bilib olishga imkon beradi |
| B. SOCl mutahassislari tobora murakkablashib borayotgan hujumlarning oldini olish va ularga samarali javob berish uchun raqamli sud ekspertizasi,  zararli dasturlarni tahlil qilish |
| C. Ichki tahdidlar toʻgʻrisidagi maʻlumotlar, ommaviy axborot manbalaridan  olingan tahlillar |
| D. Toʻgʻri qurilgan hodisaga javob berish jarayoni, bu zararni cheklash va  oqibatlarini bartaraf etish xarajatlarini kamaytirish imkonini beradi |

№27 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidlarni tahlil qilish uchun asosiy SOC elementi, yaʻni toʻgri tuzilgan  jarayon bu - … |
| A. Toʻgʻri qurilgan hodisaga javob berish jarayoni, bu zararni cheklash va  oqibatlarini bartaraf etish xarajatlarini kamaytirish imkonini beradi |
| B. SOC mutahassislari tobora murakkablashib borayotgan hujumlarning oldini olish va ularga samarali javob berish uchun raqamli sud ekspertizasi,  zararli dasturlarni tahlil qilish |
| C. Ichki tahdidlar toʻgʻrisidagi maʻlumotlar, ommaviy axborot manbalaridan  olingan tahlillar |
| D. Anʻanaviy himoya vositalari (xavfsizlik devorlari, hujumlarni aniqlash va oldini olish tizimlari, SIEM va boshqalar) bilan aniqlab boʻlmaydigan zararli  harakatlar haqida oldindan bilib olishga imkon beradi |

№28 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidli maʻlumotlar oqimlaridagi maʻlumotlarni tematik guruhlaridan biri -  IP va URL manzillar… |
| A. Zararli va fishing saytlarining tarmoq identifikatorlari, shuningdek, botnet  C&C serverlari (jumladan, mobil qurilmalar uchun) mavjud. |
| B. Tegishli maʻlumotlar eng xavfli va keng tarqalgan zararli dasturlarni, shu  jumladan mobil operatsion tizimlar uchun infektsiyalarni qamrab oladi. |
| C. Ular uchinchi tomon yechimlari va xizmatlari tomonidan foydalanish  mumkin boʻlgan ishonchli fayllar xeshlarini oʻz ichiga oladi. |
| D. xavfsizlik strategiyasini moslashtirish orqali himoya choralarini yaxshilash  imkonini beradi |

№29 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidli maʻlumotlar oqimlaridagi maʻlumotlarni tematik guruhlaridan biri -  Zararli obʻektlar xeshlari … |
| A. Tegishli maʻlumotlar eng xavfli va keng tarqalgan zararli dasturlarni, shu  jumladan mobil operatsion tizimlar uchun infektsiyalarni qamrab oladi. |
| B. Zararli va fishing saytlarining tarmoq identifikatorlari, shuningdek, botnet  C&C serverlari (jumladan, mobil qurilmalar uchun) mavjud. |
| C. Ular uchinchi tomon yechimlari va xizmatlari tomonidan foydalanish  mumkin boʻlgan ishonchli fayllar xeshlarini oʻz ichiga oladi. |
| D. xavfsizlik strategiyasini moslashtirish orqali himoya choralarini yaxshilash  imkonini beradi |

№30 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidli maʻlumotlar oqimlaridagi maʻlumotlarni tematik guruhlaridan biri –  Oq roʻyhatga olish … |
| A. Ular uchinchi tomon yechimlari va xizmatlari tomonidan foydalanish  mumkin boʻlgan ishonchli fayllar xeshlarini oʻz ichiga oladi. |
| B. Zararli va fishing saytlarining tarmoq identifikatorlari, shuningdek, botnet |

|  |
| --- |
| C&C serverlari (jumladan, mobil qurilmalar uchun) mavjud. |
| C. Tegishli maʻlumotlar eng xavfli va keng tarqalgan zararli dasturlarni, shu  jumladan mobil operatsion tizimlar uchun infektsiyalarni qamrab oladi. |
| D. xavfsizlik strategiyasini moslashtirish orqali himoya choralarini yaxshilash  imkonini beradi |

№31 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| … - tashqaridan foydalanish mumkin boʻlgan mamlakat veb-resurslarining  xavfsizlik holatini aniqlash va tahlil qilish yoʻli bilan tuziladi. |
| A. Tahdid vektorlari roʻyxati |
| B. Zararli dasturlar va kiberhujumlarni tahlil qilish |
| C. Oldindan shartlarni aniqlash |
| D. Retrospektiv tahlil |

№32 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| … - Kasperskiy laboratoriyasining noyob manbalaridan olingan ichki  monitoring maʻlumotlari asosida maʻlum bir mamlakatga qaratilgan zararli dasturlar va kiberhujumlarni tahlil qilish. |
| A. Zararli dasturlar va kiberhujumlarni tahlil qilish |
| B. Tahdid vektorlari roʻyxati |
| C. Oldindan shartlarni aniqlash |
| D. Retrospektiv tahlil |

№33 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| … - muayyan mamlakatda maʻlumotlarning sizib chiqishi uchun zaruriy  shartlarni aniqlash. |
| A. Oldindan shartlarni aniqlash |
| B. Tahdid vektorlari roʻyxati |
| C. Zararli dasturlar va kiberhujumlarni tahlil qilish |
| D. Retrospektiv tahlil |

№34 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| … - obuna davrida avval chiqarilgan barcha yopiq hisobotlarga kirish  imkoniyati taqdim etiladi. |
| A. Retrospektiv tahlil |
| B. Tahdid vektorlari roʻyxati |
| C. Zararli dasturlar va kiberhujumlarni tahlil qilish |
| D. Oldindan shartlarni aniqlash |

№35 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Threat Hunting nima? |
| A. Tahdidlarni ovlash |
| B. Tahdid vektorlari roʻyxati |
| C. Tahdidlarni aniqlash |
| D. Tahdidlarni oldini olish |

№36 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Threat Hunting nechta bosqichdan iborat? |
| **A. 2** |
| B. 3 |
| C. 4 |
| D. 5 |

№37 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Threat Hunting bosqichlari nimadan iborat? |
| A. Gipotezani shakllantirish va gipotezani tekshirish |
| B. Gipotezani tekshirish va gipotezani tasdiqlash |
| C. Gipotezani aniqlash va gipotezani tekshirish |
| D. Gipotezani tekshirish va gipotezani tugallash |

№38 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdid razvedkasi nima? |
| Tahdid razvedkasi, shuningdek, nomi bilan tanilgan kiber tahdid razvedkasi  tashkilotga qarshi mavjud yoki potentsial hujumlar toʻgʻrisida bir qator manbalardan toʻplangan maʻlumotlar. |
| Intellektual mulkni oʻgʻirlash |
| Neytral neytrallik Internet nomlari va raqamlari |
| Potentsial hujumlar toʻgʻrisida audio maʻlumotlar chiqib ketishi |

№39 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdid razvedkasining asosiy maqsadi-….. |
| Tashkilotlarga tashqi tahdidlardan kelib chiqadigan turli xil xavflarni  koʻrsatishdir |
| Signal boʻyicha yoki oʻrnatilgan vaqtda harakatga keltirish |
| Telekommunikatsiya tarmoqlarida axborot almashinuvini bostirish vositalari, |
| davlat va harbiy boshqaruv kanallarida axborotni soxtalashtirish |

№40 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Kiberxavfsizlik sohasi bu ? |
| Hisoblashga asoslangan bilim sohasi boʻlib, buzgʻunchilar mavjud boʻlgan sharoitda amallarni kafolatlash uchun oʻzida texnologiya, inson, axborot va  jarayonni mujassamlashtirgan. |
| Hisoblashga asoslangan bilim sohasi boʻlib, kirishni cheklamaydigan  qoidalarni belgilaydi |
| Maʻlumotlar oʻzgartirilmasligi, oʻchirilishi yoki noqonuniy foydalanilishi  mumkin emasligini bildiradi va kirishni cheklaydigan qoidalarni belgilamaydi. |
| davlat va harbiy boshqaruv kanallarida axborotni soxtalashtirish |

№41 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| * Kiber mojarolar ? |
| * Intellektual mulkni oʻgʻirlash * Kiber josuslik * Kiber -sabotaj * Kiber urush |
| * Zararkunanda dasturlar * Oʻzini oshkor qilish * Tegishli tizimdan foydalanish |
| * Kiber jinoyatchilik * Geolokatsiya * Maxfiylik |
| * Tegishli tizimdan foydalanish * Kiber jinoyatchilik |

№42 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Kiberxavfsizlikning uchta asosiy terminlari qaysilar? |
| Konfidentsiallik, yaxlitlik va mavjudlik |
| Konfidentsiallik, aniqlilik va ishonchlilik |
| Yaxlitlik, tushunarlilik va ishonchlilik |
| Mavjudlik, tushunarlilik va yaxlitlik |

№43 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| …. Nima uchun tahdid razvedkasi muhim |
| Harbiy, biznes yoki xavfsizlik sharoitida razvedka-bu tashkilotni qarorlarni  qoʻllab-quvvatlash va ehtimol strategik ustunlikni taʻminlaydigan maʻlumot |
| Bu vaqt davomida maʻlumotlarning izchil, aniq va ishonchli ekanligiga  ishonch hosil qiladi. |
| Dasturiy taʻminot, tarmoqlar, qurilmalar va xavfsizlik uskunalari kabi barcha |

|  |
| --- |
| zarur komponentlarning mavjudligi taʻminlanishi va yangilanishi kerak |
| Signal boʻyicha yoki oʻrnatilgan vaqtda harakatga keltirish maqsadida harbiy  yoki fuqaro infrastrukturalariga oʻrnatiluvchi dasturlangan qurilmalar |

№44 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Butunlik-…. |
| Bu vaqt davomida maʻlumotlarning izchil, aniq va ishonchli ekanligiga  ishonch hosil qiladi. |
| U maʻlumotlarga kirishni cheklaydigan qoidalarni belgilaydi. Maxfiylik  maxfiy maʻlumotlarni kiberhujumchilar va xakerlarga kirishni cheklash choralarini koʻradi |
| Dasturiy taʻminot, tarmoqlar, qurilmalar va xavfsizlik uskunalari kabi barcha  zarur komponentlarning mavjudligi taʻminlanishi va yangilanishi kerak |
| Signal boʻyicha yoki oʻrnatilgan vaqtda harakatga keltirish maqsadida harbiy  yoki fuqaro infrastrukturalariga oʻrnatiluvchi dasturlangan qurilmalar |

№45 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Mavjudligi-… |
| Dasturiy taʻminot, tarmoqlar, qurilmalar va xavfsizlik uskunalari kabi barcha  zarur komponentlarning mavjudligi taʻminlanishi va yangilanishi kerak |
| Signal boʻyicha yoki oʻrnatilgan vaqtda harakatga keltirish maqsadida harbiy  yoki fuqaro infrastrukturalariga oʻrnatiluvchi dasturlangan qurilmalar |
| Bu vaqt davomida maʻlumotlarning izchil, aniq va ishonchli ekanligiga  ishonch hosil qiladi. |
| U maʻlumotlarga kirishni cheklaydigan qoidalarni belgilaydi. Maxfiylik maxfiy maʻlumotlarni kiberhujumchilar va xakerlarga kirishni cheklash  choralarini koʻradi |

№46 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Kiber tahdid tahlilchisi? |
| Kiber tahdid tahlilchisi tizimning zaifligini aniqlash, potentsial tahdidlarni  kuzatish va baholash va tarmoqning xavfsizlik talablariga javob berishini taʻminlashdir |
| Maʻlumotlarning ishonchli ekanligiga ishonch hosil qiladi va javob bermaydi. |
| Dasturiy taʻminot, tarmoqlar, qurilmalar va xavfsizlik uskunalari kabi barcha  zarur komponentlarning mavjudligi taʻminlanishi va yangilanishi kerak |
| Signal boʻyicha yoki oʻrnatilgan vaqtda harakatga keltirish maqsadida harbiy  yoki fuqaro infrastrukturalariga oʻrnatiluvchi dasturlangan qurilmalar |

№47 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Intellektual inqilob natijasida ……-yillardan eʻtiboran davlatlar kiberdunyo taqdim etgan imkoniyatlardan oʻz harbiy salohiyatlarini rivojlantirish yoʻlida  ham foydalana boshladilar.? |

|  |
| --- |
| 1990 |
| 1997 |
| 1998 |
| 1991 |

№48 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Strategik tahdid razvedka? |
| Ushbu tahlil potentsial kiberhujumlarni va manfaatdor tomonlar, shuningdek  qaror qabul qiluvchilar uchun mumkin boʻlgan oqibatlarni umumlashtiradi |
| Fizik interfeys, paket qaerdan keladi; Manbaning IP manzili; Qabul  qilmaydigan IP manzili; |
| Maʻlumotlarning ishonchli ekanligiga ishonch hosil qiladi va javob bermaydi. |
| Dasturiy taʻminot, tarmoqlar, qurilmalar va xavfsizlik uskunalari kabi barcha  zarur komponentlarning mavjudligi taʻminlanishi va yangilanishi kerak |

№49 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Taktik tahdid razvedka? |
| Taktik razvedka tahdid koʻrinishlaridan foydalanadigan taktika, texnika va  protseduralar haqida maʻlumot beradi |
| Signal boʻyicha yoki oʻrnatilgan vaqtda harakatga keltirish |
| Telekommunikatsiya tarmoqlarida axborot almashinuvini bostirish vositalari, |
| davlat va harbiy boshqaruv kanallarida axborotni soxtalashtirish |

№50Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Texnik tahdid razvedka? |
| Ushbu maʻlumot hujum boshlanganligini koʻrsatadigan belgilarga qaratilgan |
| Signal boʻyicha yoki oʻrnatilgan vaqtda harakatga keltirish |
| Telekommunikatsiya tarmoqlarida axborot almashinuvini bostirish vositalari, |
| davlat va harbiy boshqaruv kanallarida axborotni soxtalashtirish |

№51 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Operatsion tahdid razvedka? |
| Ushbu yondashuv bilan maʻlumotlar turli xil manbalardan, ijtimoiy tarmoqlar, antivirus jurnallari va oʻtgan voqealardan toʻplanadi. |
| Ushbu TE lar bogʻlanish oʻrnatishdan keyin tarmoq paketlarini aynan amaliy  sathga mosligini baholaydi. |
| Ushbu tahlil potentsial kiberhujumlarni va manfaatdor tomonlar, shuningdek  qaror qabul qiluvchilar uchun mumkin boʻlgan oqibatlarni umumlashtiradi |
| Fizik interfeys, paket qaerdan keladi; Manbaning IP manzili; Qabul |

|  |
| --- |
| qilmaydigan IP manzili; |

№52 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdid razvedkasining hayot aylanishi |
| Tahdid razvedkasining hayot aylanishi tahdid razvedkasi guruhlari uchun  xavfsizlik choralarini yanada samarali belgilash va amalga oshirish uchun asos boʻlib xizmat qiladi. |
| Ushbu tahlil potentsial kiberhujumlarni va manfaatdor tomonlar, shuningdek  qaror qabul qiluvchilar uchun mumkin boʻlgan oqibatlarni umumlashtiradi |
| Fizik interfeys, paket qaerdan keladi; Manbaning IP manzili; Qabul  qilmaydigan IP manzili; |
| Ushbu TE lar bogʻlanish oʻrnatishdan oldin va keyin tarmoq paketlarini aynan  amaliy sathga mosligini baholaydi. |

№53 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidlarni necha guruhga ajratish mumkin? |
| 6 |
| 3 |
| 4 |
| 5 |

№54 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Oʻz DSt 1106:2009 yilda qanday standart ishlab chiqilgan? |
| «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash  funksiyasi»; |
| «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron  raqamli imzoni shakllantirish va tekshirish jarayonlari»; |
| «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elliptik egri  chiziqlarga asoslangan elektron raqamli imzoni shakllantirish va tekshirish jarayonlari». |
| «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Kriptografik  modullarga oid xavfsizlik talablari »; |

№55 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Oʻz DSt 1108:2009 yilda qanday standart ishlab chiqilgan? |
| «Axborot texnologiyasi. Ochiq tizimlar oʻzaro bogʻliqligi. ERI ochiq kaliti  sertifikati va atribut sertifikatining tuzilmasi»; |
| «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Kriptografik  modullarga oid xavfsizlik talablari »; |
| «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elliptik egri  chiziqlarga asoslangan elektron raqamli imzoni shakllantirish va tekshirish |

|  |
| --- |
| jarayonlari». |
| «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Kriptografik  modullarga oid xavfsizlik talablari »; |

№56 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidlarni yuzaga kelish sabablariga kura :? |
| -ehtimoliy tahdid,-ehtimol boʻlmagan tahdid. |
| -Ehtimoli boʻlgan tahdidlar ,-tabiiy ofatlar |
| -qasddan qilingan tahdidlar. |
| -ichki tahdidlar |

№57 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| … - bu kompyuterlar, tarmoqlar yoki ular saqlangan maʻlumotlarga qarshi kompyuterga asoslangan hujumni boshlash orqali hukumatni yoki tashkilotni siyosiy yoki ijtimoiy maqsadlarini ilgari surish uchun qoʻrqitadigan yoki majburlaydigan kishi. |
| Kiberterrorist |
| Kiberetika |
| Kibertahdid |
| Kibermakon |

№58 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Necha foiz tahdid tashqi tomondan kelib chiqishi mumkin? |
| 17% |
| 21% |
| 16% |
| 30% |

№59 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidlarning necha foizi tasodifiy shaxslar tomonidan amalga oshiriladi? |
| 1% |
| 2% |
| 5% |
| 3% |

№60 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Simsiz mobil tarmoqlarning xavfsizligini nechta asosiy xizmat taʻminlab |

|  |
| --- |
| beradi? |
| 3 |
| 4 |
| 2 |
| 5 |

№61 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Korxona (firma, kompaniya va boshqalar) ning xavfsizlik xizmati tarkibi, hajmi va tarkibi.) korxonaning real yehtiyojlari va axborotlarining maxfiyligi  qanday baholanadi? |
| Darajasi qarab |
| Turiga qarab |
| Toʻri javob yoʻq |
| Hajmiga qarab |

№62 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Korxona xavfsizlik xizmatining asosiy vazifalari |
| Korxona xavfsizligini taʻminlash |
| Ishlab c hodimlarni nazorat qilish |
| mahsulot sifatini tekshirish |
| Toʻgʻri javob yoʻq |

№63Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| SSL/TLS ulanishlarni …………………va uchun ishlatiladi. |
| Autentifikatsiyalash va shifrlash |
| Identifikatsiyalash va shifrlash |
| Himoyalash va shifrlash |
| Autentifikatsiyalash va identifikatsiyalash |

№64 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| …………. - bu dasturlar va operatsion tizimning muhim dasturiy va tadbirlari  toʻgʻrisidagi maʻlumotlarni yozib olish va markazlashtirish uchun standart usul.? |
| Hodisalarni (voqea) yozib boorish |
| Dastur ish faoliyatida boʻlmaganda hodisalarni (voqea) yozib boorish |
| Markazlashmagan tizimlarda boʻlmaganda hodisalarni (voqea) yozib boorish |
| Barcha javoblar notoʻgʻri |

№65 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Kirish nazorati-bu …… |
| subʻektning haqiqiyligini aniqlash va kirish haqiqatini qayd yetish. |
| himoya obʻekti atrofida baʻzi yopiq chegaralarni yaratishdir. |
| joʻnatuvchini boshqa abonent qiyofasida koʻrsatish |
| foydalanuvchi tizimga kiradigan terminalni autentifikatsiyalashdir. |

№66 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot portreti- bu…… |
| xabar (nutq yoki maʻlumotlar) maʻnosini, obʻekt yoki signal xususiyatlarini  aks ettiruvchi elementlar va ular orasidagi bogʻlanishlar toʻplamidir. |
| Kuzatish obʻektlari, signallari va moddalarining axborot portretlari ularning  mos yozuvlar xususiyati tuzilmalari hisoblanadi. |
| portretning axborot tugunini ( maʻlumot beruvchi qismini) tashkil etuvchi  baʻzi elementlar va havolalarni olib tashlash. |
| ularning sonini saqlab turgan holatda axborot portreti elementlari orasidagi  bogʻlanishlarni oʻchirish yoki oʻzgartirish. |

№67 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tajovuzkor tomonidan toʻgʻridan-toʻgʻri tinglash qanday fazifalarni oʻz  ichiga oladi? |
| maxfiy eshitish va yodlash; maxfiy eshitish va yozib olish. |
| maxfiy eshitish va yodlash; yozib olish |
| Oshkora koʻrish va maxfiy yozib olish |
| Oshkora koʻrish va maxfiy yozib olish |

№68 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Maʻlumotni tiklash texnikasi? |
| Bu kompyuterda yoʻq qilingan, foydalanib boʻlmaydigan, buzilgan yoki formatlangan maʻlumotlarni, saqlanishda, ularda saqlangan maʻlumotlarga  kirishning iloji boʻlmaganda tiklash jarayoni |
| Bu kompyuterda yoʻq qilinmagan, foydalanib boʻlmaydigan, buzilgan yoki formatlangan maʻlumotlarni, saqlanishda, ularda saqlangan maʻlumotlarga  kirishning iloji boʻlmaganda tiklash jarayoni |
| Bu kompyuterda yoʻq qilingan, foydalanib boʻladigan, buzilgan yoki formatlangan maʻlumotlarni, saqlanishda, ularda saqlangan maʻlumotlarga  kirishning iloji boʻlmaganda tiklash jarayoni |
| Bu kompyuterda yoʻq qilingan, foydalanib boʻlmaydigan, buzilgan yoki formatlangan maʻlumotlarni, saqlanishda, ularda saqlangan maʻlumotlarga  kirishning iloji boʻlganda tiklash jarayoni |

№69 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |  |
| --- | --- |
| Mustaqillik yillarida qabul qilingan Oʻzbekiston Respublikasining  «Avtomatlashtirilgan bank tizimida axborot muhofazasi toʻgʻrisidagi» qonun va farmonlari qachon qabul qilingan? | |
| 2005 yil | 16 noyabr |
| 2006 yil | 16 noyabr |
| 2004 yil | 16 noyabr |
| 2000 yil | 16 noyabr |

№70 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Мaʻlumotni yoʻqotish xavfi hamma uchun bir xilmi? |
| Bir xil |
| Bir xil emas |
| Barchasida har xil |
| Individual |

№71 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot xavfsizligida tahdid nima? |
| texnik vositalar bilan ishlov berilganda axborotning asosiy sifat  xususiyatlarini buzish salohiyati |
| Maxfiy maʻlumotlar bilan uning yaxlitligini buzmagan holda turli usul va  yoʻllar bilan tanishish |
| Axborotni noqonuniy harakatlar bilan yuq qilish |
| himoyalangan axborotni noqonuniy ravishda sotib olish |

№72 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Eng yaxshi bepul bulutli zaxiralash xizmatlari? |
| IDrive. ICloud. Degoo. |
| IDrive. ICloud. Docx. |
| IDrive. Docx. Degoo. |
| Docx. ICloud. Degoo. |

№73 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Differentsial zaxira? |
| Differentsial zaxira kengaytirilgan zaxiralash.. |
| Differentsial zaxira kengaytirilmagan zaxiralash.. |
| Differentsial zaxira kengaytirilmagan tiklash.. |
| Differentsial zaxira kengaytirilgan va kengaytirilmagan zaxiralash.. |

№74 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Ichki tahdid manbalarini sanab oʻting: |
| * korxona maʻmuriyati; * xodimlar; * ishlab chiqarish va mehnatni taʻminlashning texnik vositalari faoliyati. |
| * adolatsiz raqobatchilar; * jinoiy guruhlar va tuzilmalar; * maʻmuriy-boshqaruv shaxslari va tashkilotlari apparati. |
| * faol; * passiv; |
| * material; * ahloqiy; |

№75 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdid nima ? |
| maʻnaviy yoki moddiy zarar yetkazadigan potentsial yoki haqiqiy harakat. |
| texnik vositalar bilan ishlov berilganda axborotning asosiy sifat xususiyatlari  (xususiyatlari) ni buzish salohiyati: |
| jinoiy maqsadlar uchun axborotni axborot tarkibi va mazmunining qisman  yoki sezilarli oʻzgarishi sifatida oʻzgartirish; |
| bevosita moddiy zarar yetkazish maqsadida axborotni yoʻq qilish (yoʻq  qilish). |

№76 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot aktivlarini hayotiy davrini boshqarish nima? |
| axborot korhona ichida foydalanilganda uni boshqarish xavsizligini taminlash |
| korhona ichida pul mablagʻlarini boshqarish |
| Dasutiy taʻminotini qoʻriqlash |
| Barcha javoblar toʻgʻri |

№77 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Android-antiviruslar ikkita parametrga asoslaymiz bular qaysilar? | | | | | |
| Himoya – tahdidlarni samarali qurilmaning ishlashiga taʻsiri. | | | aniqlash | qobiliyati, Yuzabiliti – | mobil |
| Himoya – tahdidlarni samarali aniqlamaydigan qobiliyati, Yuzabiliti – mobil  qurilmaning ishlashiga taʻsiri. | | | | | |
| Himoya –  qurilmaning | tahdidlarni  taʻsiri. | samarali | aniqlash | qobiliyati, Hujum – | mobil |
| Himoya – | tahdidlarni | samarali | aniqlash | qobiliyati, tizimli – | mobil |

|  |
| --- |
| qurilmaning ishlashiga taʻsiri. |

№78 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| …….. - bu xavfsizlikni boshqarish vositalarining (xavfsizlikka qarshi choralar) joylashishini va ularning umumiy tizim arxitekturasiga qanday  aloqadorligini tasvirlaydigan dizayn artefaktlari. |
| Xavfsizlik arxitekturasi |
| Xavfsizlik siyosati |
| Xavfsizlik darajasi |
| Xavfsizlik turlari |

№79 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| …. — bu ularning ishlash tamoyili ћar bir tekshiriluvchi obʻektdan (fayldan,  yuklovchi sektordan, tizimli reestrdan) nazorat summasini oʻqib olib, uni tegishli maʻlumotlar bazasida saqlashdan iborat. |
| Oʻzgarishlarni qayd qiluvchi revizorlar |
| Skanerlar |
| virus ћarakatini cheklovchi blokiratorlar |
| Barcha javoblar toʻgʻri |

№80 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| …… - bu subʻektlar bir-biriga qanday kirishlari, turli subʻektlar qanday operatsiyalarni amalga oshirishi, tizim yoki dasturiy mahsulot uchun qanday himoya darajasi talab qilinishi va ushbu talablar bajarilmasa qanday harakatlar  qilinishi kerakligi bayonati berilganligi. |
| Xavfsizlik siyosati |
| Xavfsizlik arxitekturasi |
| Xavfsizlik darajasi |
| Xavfsizlik turlari |

№81 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Ogohlantirish moslamalari nima uchun kerak? |
| Annunciatorlar yorugʻlik va ovozli signallarni berish, xavfsizlik xodimlari  eʻtiborini jalb qilish va huquqbuzarga psixologik taʻsir oʻtkazish uchun |
| detektorlar va uzatish liniyalari (koʻchadan) holati toʻgʻrisida maʻlumot  toʻplash va qayta ishlashga |
| bino ichidagi yuqori haroratni aniqlash uchun |
| Xavfsizlik siyosati |

№82 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Framework bu - ? |
| dasturiy tizimning tuzilishini belgilaydigan dastur; yirik dasturiy taʻminot loyihasining turli xil tarkibiy qismlarini ishlab chiqish va birlashtirishga yordam  beradigan dastur. |
| dasturiy tizimning tuzilishini belgilaydigan dastur; yirik dasturiy taʻminot loyihasining turli xil tarkibiy qismlarini ishlab chiqish va birlashtirishga yordam  bermaydigan dastur. |
| bu korxona xavfsizligi arxitekturasi va xizmatlarini boshqarish uchun asos va  uslubidir. |
| IT (axborot texnologiyalari) boshqaruviga yoʻnaltirilgan xalqaro professional  birlashma. |

№83 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| SABSA (Sherwood Applied Business Security Architecture) qanday  xavfsizlik arxitekturasi ? |
| amaliy xavfsizlik arxitekturasi |
| nazariy xavfsizlik arxitekturasi |
| amaliy va nazariy xavfsizlik arxitekturasi |
| Barcha javoblar notoʻgʻri |

№84 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yuqotilishiga toʻsqinlik qiluvchi tashkiliy,  texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi - ? |
| axborotni himoyalash tizimi |
| axborotni buzish tizimi |
| axborotni tashkil qiluvchi tizimi |
| axborotni zaif tomonlarini kamaytiruvchi tizimi |

№85 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tarmoqlararo ћimoya ekrani inglizcha nomini toping |
| FireWall |
| Network |
| Xavfsiz tarmoq |
| Brandmauer tarmoq |

№86 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Xavf-xatarni taxlillash bu..... |
| tarmogining zaif elementlari taxlil- lanadi, takdidlar anikdanadi va  bakolanadi, himoyaning optimal vositalari tanlanadi |

|  |
| --- |
| xavfsizlik siyosatini amalga oshirish moliyaviy xarajatlarni kisoblash va  masalalarni yechish uchun mos vositalarni tanlash bilan boshlanadi |
| utkaziladigan tadbirlar niyati buzuk odamlarning tarmokka bostirib kirishini doimo nazorat kilib turishni, axborot obʻektini himoyalash tizimidagi “rakna”larni anikdashni, konfidentsial maʻlumotlardan ruxsatsiz foydalanish  kollarini kisobga olishni talab etadi |
| xavfsizlikning muayyan tizimi buzilishining barcha xollariga operativ munosabat bildirishi, ularni taxlillashi va moliyaviy vositalarning maksimal  tejalishini kisobga olgan kolda himoyaning zaruriy apparat va dasturiy vositalaridan foydalanadi |

№87 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborotlarni tashkiliy himoyalash elementlari qanday bogʻlovchi omil boʻlib  hisoblanadi? |
| yagona tizimga |
| sanoqli tizimga |
| sanoqsiz tizimga |
| Barcha javoblar notoʻgʻri |

№88 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axbortlarni himoyalashning tashkiliy chora – tadbirlari tashkilot xavfsizligi  xizmatining nimalarda oʻz aksini topadi? |
| meʻyoriy uslubiy hujjatlarida |
| tashkiliy uslubiy hujjatlarida |
| texnik uslubiy hujjatlarida |
| Barcha javoblar notoʻgʻri |

№89 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborotni himoyalashning dasturiy – matematik elementi kompyuter, lokal tarmoq va turli axborot tizimlarida qayta ishlanadigan va saqlanadigan qimmatli  axborotlarni nima qilish uchun moʻljallangan |
| Himoyalash |
| Skanerlash |
| Filtrlash |
| Tekshirish |

№90 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Kompyuter tizimi (tarmogi)ga ziyon yetkazishi mumkin boʻlgan sharoit,  harakat va jarayonlar uchun nima hisoblanadi. |
| xavf – xatarlar |

|  |
| --- |
| Himoya va hatarlar |
| Xavfsizlik tizimi |
| Barcha javoblar notoʻgʻri |

№91 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Audit nima? |
| Tashkilotda axborot xavfsizligini boshqarish boʻyicha tadbirlarni amalga oshirish ishlab chiqilgan reja asosida yoxud xavfsizlik boʻyicha tadbirlarni  amalga oshirishda katta oʻzgarishlar yuz berganida mustaqil tekshirilishi |
| Hisobotlarni tekshirish |
| Taftish oʻtkazish |
| Bosh tashkilot tomonidan nazoratni kuchaytirish |

№92 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Ishonchsiz xodim kim? |
| oʻzining harakatlari bilan sanoat josusi yetkazadigan muammoga teng (undan  ham koʻp boʻlishi mumkin) muammoni toʻgdiradi |
| boshqa kompьyuter qaroqchilaridan farqli holda, baʻzida, oldindan, maqtanish  maqsadida kompьyuter egalariga ularning tizimiga kirish niyatlari borligini  bildirib qoʻyadilar |
| elektron “oʻgrilar” manfaatmaqsadida dasturlarni buzishga ixtisoslashganlar |
| raqobat qiluvchi firmalar va xatto ajnabiy maxsus xizmatlari buyurtmasi  boʻyicha axborotni oʻgirlovchi firma va kompaniyalarning yuqori malakali mutaxassislari |

№93 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Xavflarni boshqarish bu...... |
| xavf xatarlarga qarshi chora va tadbirlarni qoʻllab quvvatlash shu bilan birga  ularning xavfsizlik tizimlariga boʻlgan taʻsirlarini normal darajada kamaytirish jarayoni |
| maʻlumotlar yashirilgan, oʻzgartirilgan, oʻchirilgan yoki foydalanishni  ruxsatsiz qilinganligi; |
| qurilmalarning buzilishi yoki shikastlanishi;. |
| dasturiy taʻminotni butunligini buzilishi natijasida kelib chiqishi mumkin |

№94 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot texnologiyalari xavfi yoki IT-xavf – bu? |
| Axborot texnologiyalaridan foydalanish bilan bogʻliq har qanday xavf |
| Turli xil hodisalarning yuzaga kelish ehtimoli |

|  |
| --- |
| IT xavfini baholash |
| Zaifliklar va aktivlar hajmi kabi bogʻliq omillarni baholash |

№95 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |  |
| --- | --- |
| IT xavflarini oʻlchashning alternativ usullari odatda nimalarni uz ichiga oladi? | |
|  | Tahdidlar, zaifliklar va aktivlar hajmi kabi bogʻliq omillarni baholashni oʻz |
| ichiga oladi | |
| Axborot texnologiyalaridan foydalanish bilan bogʻliq har qanday xavf | |
| Turli xil hodisalarning yuzaga kelish ehtimoli | |
| Zaifliklar va aktivlar hajmi kabi bogʻliq omillarni baholash | |

№96 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Xavfni minimallashtirish – bu? |
| tashkilot uchun umumiy xavfni kamaytirish uchun choralar koʻrish |
| Tahdidlar, zaifliklar va aktivlar hajmi kabi bogʻliq omillarni baholashni oʻz  ichiga oladi |
| Axborot texnologiyalaridan foydalanish |
| Turli xil hodisalarning yuzaga keltirish |

№97 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Qaysi yilning 3 apreldagi «OʻzRda axborotning kriptografik muhofazasini tashkil etish chora-tadbirlari toʻgʻrisida» PQ-614–son qarorining asosiy  vazifalaridan biri hisoblanadi? |
| 2007 |
| 2008 |
| 2009 |
| 2010 |

№98 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Kompyuter kriptografiyasi davrining birinchi muhim voqeasi simmetrik  kriptotizimlarning birinchi sinfi boʻlgan qanday shifrlar yuzaga keladi? |
| Blokli |
| Blokli va bloksiz |
| Bloksiz |
| Blokli simmetrik |

№99 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Zaifliklarni tatbiqiy hamda tizimli sathlarda tezdan samarali qidirishni amalga  oshiruvchi tarmoq xavfsizligi skaneri. Ushbu skaner har qanday koʻlamli |

|  |
| --- |
| tarmoqlarda xavfsizlik maqomini nazoratlashning samarali tizimini barpo etadi.  Bu qanday Himoyalanganlikni taxlillovchi dastur? |
| XSpider 7.8 |
| Tarmoq revizori |
| Tarmoqlararo ekran texnologiyasi |
| Bitlocker |

№100 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Identifikatsiya (Identification) - ? |
| foydalanuvchini uning identifikatori (nomi) boʻyicha aniqlash jarayoni |
| foydalanuvchini uning identifikatori (nomi) boʻyicha aniqlanmaydigan  jarayoni. |
| foydalanuvchini uning identifikatori (paroli) boʻyicha aniqlash jarayoni |
| foydalanuvchini uning autentifikatsiyasi (nomi) boʻyicha aniqlash jarayoni |

№101 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| ruxsatsiz foydalanishga urinishlarni bartaraf etishga moʻljallangan tarmoq skaneri. Tarmoq revizori TCP/IP steki protokollaridan foydalanuvchi oʻrnatilgan tarmoq dasturiy va apparat taʻminoti zaifliklarini aniqlash uchun ishlatiladi. Bu  qanday Himoyalanganlikni taxlillovchi dastur? |
| Tarmoq revizori |
| XSpider 7.8 |
| Skaner BC |
| bitlocker |

№102 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Foydalanuvchilarning Internetdan foydalanishlarini, trafikni qayd etishni va  filtrlashni, resurslarni tashqi xujumlardan himoyalashni tashkil etishga moʻljallangan. |
| Usergateproxy&Firewall |
| Trust access |
| Security studio endpoint protection |
| Cisco ids/ips |

№103 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| ….. — maʻlum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy  ekanligini tekshirish muolajasi.? |
| Autentifikatsiya (Authentication) |
| Autentifikatsiya (Authentication) Identification |

|  |
| --- |
| Autentifikatsiya (Identification) |
| Identification |

№104 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Oʻgʻirlangan maʻlumotlar va shu maʻlumotlarga aloqador kiber  jinoyatchilarning mahsulotlarini tarqatish va sotish? |
| Distribyutorlar |
| Jinoyatchilar |
| Tizim xostlari va provayderlari |
| Tizim xostlari |

№105 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot tizimlarida axborot xavfsizligini taʻminlashga oid raxbariyat  tomonidan qabul qilingan chora-tadbirlar qaysi bugʻinga tegishli? |
| - maʻmuriy bugʻinga |
| -huquqiy bugʻinga |
| -amaliy bugʻinga |
| -dasturiy va texnik bugʻinga |

№106 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| ISACA qanaqa tizim? |
| axborot texnologiyalarini (IT) boshqarish uchun yaratilgan tizim |
| yuklovchi sektorlar uchun tizim |
| dasturiy kodini izlash uchun yaaratilgan tizim |
| Maʻlumotlarni yuklovchi sektorlar uchun tizim |

№107 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| WLTS protokoli. Qaysi pratokollarga asoslangan? |
| SSL/TLSga asoslangan |
| SLL/TLSga asoslangan |
| SSL/LLSga asoslangan |
| SSL/TSSga asoslangan |

№108 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Internet brauzerlarda himoyalangan ulanishlar xavfsizligining muammosini  yechish uchun yaratilgan protocol? |
| SSL |
| UDP |

|  |
| --- |
| FTP |
| HTTP |

№109 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| IEEE 802.11 Wi Fi standartida qanday jarayon sodir boʻladi? |
| simsiz shaxsiy va lokal tarmoq tashkil etish |
| simli-simsiz shaxsiy va lokal tarmoq tashkil etish |
| simsiz shaxsiy va simli shaxsiy tashkil etish |
| Barcha javoblar notoʻgʻri |

№110 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| - bu maʻlumotni ruxsatsiz foydalanuvchi tomonidan osonlikcha ochib  boʻlmaydigan oʻqib boʻlmaydigan holda himoya qiladigan texnologiya? |
| Diskni shifrlash |
| Faylni shifrlash |
| Rasmni shifrlash |
| Videoni shifrlash |

№111 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot aktivlarini hayotiy davrini boshqarish nima? |
| Axborot korxona ichida foydalanilganda uni boshqarish xavfsizligini  taminlash |
| Korxona ichida pul mablagʻlarini boshqarish |
| Dasturiy taʻminotini qoʻriqlash |
| Tashkilotni tashqi himoyalash |

№112 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Uyishtirilmagan tahdid, yaʻni tizim yoki dasturdagi qurilmaning jismoniy  xatoligi – bu… |
| -Tasodifiy tahdid |
| -Uyishtirilgan tahdid |
| -Faol tahdid |
| -Passiv tahdid |

№113 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Shartli soʻz yoki shaxsni yoki vakolatni tasdiqlash uchun moʻljallangan  belgilar toʻplami? |
| Parol |

|  |
| --- |
| Login |
| Maʻmurlash |
| Autentifikatsiya |

№114 Fan bobi – 2; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| Vakolatga ega boʻlgan foydalanuvchining tarmoqqa kirishi uchun belgilangan  parol maʻlumotini qoʻlga kiritishga qaratilgan harakatlar? |
| Parollarga qaratilgan hujumlar |
| Parollarga qaratilmagan hujumlar |
| Parollarga qaratilgan imkoniyatlar |
| Loginga qaratilgan hujumlar |

№115 Fan bobi – 3; Boʻlimi – 1; Qiyinchilik darajasi – 2;

|  |
| --- |
| Autentifikatsiya jarayonida bir necha faktor ishlatilsa, bunday autentifikatsiya  bu? |
| koʻp faktorli deb yuritiladi |
| bir faktorli deb yuritiladi |
| ikki faktorli deb yuritiladi |
| faktorli deb yuritiladi |

№116 №2 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| X.509 standarti tavsiyalariga binoan qatʻiy autentifikatsiyalashning quyidagi  qaysi muolajalarda farqlanadi? |
| bir tomonlama autentifikatsiya; ikki tomonlama autentifikatsiya;  uch tomonlama autentifikatsiya; |
| bir tomonlama autentifikatsiya;  ikki tomonlama autentifikatsiya; toʻrt tomonlama autentifikatsiya; |
| bir tomonlama autentifikatsiya; ikki tomonlama autentifikatsiya;  toʻrt tomonlama autentifikatsiya; |
| bir tomonlama autentifikatsiya;  ikki tomonlama autentifikatsiya; uch tomonlama maʻmurlash; |

№117 №2 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tashkilotning tizimlari uchun foydalanuvchini identifikatsiya qilish va autentifikatsiya qilish, foydalanish huquqlari va vakolat darajalarini oʻz ichiga  olgan dasturiy taʻminotdan iborat. |
| Mantiqiy xavfsizlik nazorati |

|  |
| --- |
| Mantiqiy foydalanishni boshqarish |
| Parollarga qaratilgan hujumlar |
| Loginga qaratilgan hujumlar |

№118 Fan bobi – 3; Boʻlimi – 1; Qiyinchilik darajasi – 2;

|  |
| --- |
| Dinamik parol – ? |
| bir marta ishlatilganidan soʻng boshqa umuman ishlatilmaydigan parol |
| bir marta ishlatilmaydigan parol |
| bir marta ishlatilganidan soʻng yana ishlatiladigan parol. |
| Bir marta ishlatilgandan soʻng parolni oʻchadi |

№119 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| «Tashkilotning xavfsizlik siyosati» hujjati nima? |
| axborot xavfsizligining maqsad va prinsiplarini aniqlash uchun moʻljallangan  bulib,oʻz navbatida axborot xavfsizligi obyektlari roʻyxati koʻrsatib oʻtiladi |
| Tashkilotda yangi axborot tizimini tatbiq etish jarayonlarini beligilab oʻtish  uchun moʻljallangan |
| Tashkilotda xodimlarni tanlashda va ular bilan ishlashda axborot xavfsizligini  taʻminlash chora-tadbirlarini aniqlash uchun moʻljallangan |
| Tashkilotda yangi axborot tizimini tatbiq etish darajasini belgilash. |

№120 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| «Tashkilotning xavfsizlik siyosati» hujjati kim tomonidan tasdiqlanadi? |
| Tashkilot rahbari |
| Xavfsizlik xodimi |
| Kadrlar boʻlimi |
| Oddiy xodimlar tamonidan |

№121 Fan bobi – 3; Boʻlimi – 1; Qiyinchilik darajasi – 2;

|  |
| --- |
| Simsiz tarmoqlar xavfsizligi protokollari qaysilar? |
| LLC, SSH, SSL/TLS |
| 802.1x, SSH, SSL/TLS Dox |
| WPA , IPSec, 802.11 pdf |
| SSL/TLS , , 802.11, IEEE 802.11 Word |

№122 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| Seans sathi TE texnologiyasining kamchiliklari? |
| TSR dan boshqa protokollar ruxsatini cheklay olmaslik; Yuqori sath |

|  |
| --- |
| protokollari uchun tekshiruvni tashkil eta olmaslik; Cheklangan audit |
| Yuqori sath protokollari uchun tekshiruvni tashkil eta olmaslik; Cheklangan audit Muayyan xost bilan bogʻlanishni maʻn qilish imkoniyati; NAT dan  foydalanib-ichki IP manrzillarni bekitish |
| Qoidalarni testlash murakkabligi. Muayyan xost bilan bogʻlanishni maʻn  qilish imkoniyati; NAT dan foydalanib-ichki IP manrzillarni bekitish |
| NAT sxemasi ichki IP adreslarni “berkitadi”. Qoʻshimcha funksiyalarga  ruxsat bekmaslik-HTTP keshlash javoblari, URL ni filtrlash, autentifikatsiya |

№123 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| uMail pochta qutisini ochish qaysi tizimdan roʻyhatdan oʻtish kerak? |
| ID.uz |
| com.uz |
| IDD.uz |
| SSD.uz |

№124 Fan bobi – 3; Boʻlimi – 1; Qiyinchilik darajasi – 2;

|  |
| --- |
| Korxona ichidagi individual foydalanuvchilarning rollari asosida tarmoqqa  kirishni cheklash qaysi model? |
| RBAC modeli |
| Amazon modeli |
| Kirishni boshqarish |
| Azure modeli |

№125 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| Autentifikatsiya jarayonida faqat bitta faktor ishlatilsa, bunday  autentifikatsiya bu? |
| bir faktorli deb yuritiladi. |
| ikki faktorli deb yuritiladi. |
| Bir va ikki faktorli deb yuritiladi. |
| Ikki va uch faktorli deb yuritiladi. |

№126 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Xizmat qilishdan voz kechish hujumidan himoyalanishning eng samarali  yoʻllari quyidagilar? |
| tarmoqlararo ekranlar texnologiyasi (Firewall),  IPsec protokoli. |
| tarmoqlararo ekranlar texnologiyasi (Firewall),  IPsec protokoli, OSI modeli. |
| tarmoqlararo ekranlar texnologiyasi (Firewall), |

|  |
| --- |
| UDP Protokoli |
| TCP/IP protokollar (Firewall),  IPsec protokoli. |

№127 Fan bobi – 3; Boʻlimi – 1; Qiyinchilik darajasi – 2;

|  |
| --- |
| Ruxsatsiz kirishni aniqlash tizimi (IDS) ? |
| tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul  yoki vositalar aniqlanadi. |
| tizim yoki tarmoq xavfsizlik siyosatini buzmaydigan kirishga harakat qilingan  usul yoki vositalar aniqlanadi |
| tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul  yoki vositalar aniqlanmaydi |
| tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilinmagan usul  yoki vositalar aniqlanadi. |

№128 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| Windows jurnallari-…..? |
| Operatsion tizim tomonidan ilovalar, tizim komponentlari, xavfsizlik va ishga tushirish bilan bogʻliq tizimga oid voqealarni roʻyhatdan oʻtkazish uchun  foydalaniladi. |
| Dasturlar va operatsion tizimning muhim dasturiy va tadbirlari toʻgʻrisidagi  maʻlumotlarni yozib olish va markazlashtirish uchun standart usul. |
| Ilovalar va xizmatlar tomonidan ularning ishlariga taalluqli voqealarni yozish  uchun ishlatiladi. |
| davomiylikning buzilishi bilan bogʻliq qabul qilinishi mumkin boʻlmagan  oqibatlarga yoʻl qoʻymasdan jarayonni tiklash jarayonidir hamda xizmat koʻrsatish. |

№129 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| «Tashkilotning xavfsizlik siyosati» hujjati shakli qanday koʻrinishda boʻladi |
| Nizom |
| Yoʻriqnoma |
| Maʻlumotnoma |
| Ogʻzaki |

№130 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| Mak-Elis kriptotizimida qanday tuzatuvchi kodlar ishlatiladi? |
| Xatoliklarni tuzatuvchi kodlar ishlatiladi |
| Xatoliklarni tuzatuvchi kodlar ishlatilmaydi |
| Xatoliklarni tuzatmaydigan kodlar ishlatiladi |

|  |
| --- |
| Barcha javoblar notoʻgʻri |

№131 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul  yoki vositalar aniqlanadi? |
| Ruxsatsiz kirishni aniqlash tizimi |
| Ruxsatli kirishni aniqlash tizimi |
| Ruxsatsiz kirishni aniqlash fayli |
| Ruxsatsiz chiqishni aniqlash tizimi |

№132 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| Ruxsatsiz kirishni aniqlash tizimi qisqartirilgan nomini aniqlang ? |
| IDS |
| IBD |
| ISD |
| IIS |

№133 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Qayd etish tizimda nima deyiladi? |
| Maʻmurlash |
| Tasdiqlash |
| Tekshirish |
| Yuqotish |

№134 Fan bobi – 3; Boʻlimi – 1; Qiyinchilik darajasi – 2;

|  |
| --- |
| Konfidentsiallik, yaxlitlik va mavjudlik bu kiberxavfsizlikning qancha asosiy  tushuchalari bor ? |
| Kiberxavfsizlikning uchta asosiy tushuchalari |
| Kiberxavfsizlikning oltita asosiy tushuchalari |
| Kiberxavfsizlikning toʻrtta asosiy tushuchalari |
| Kiberxavfsizlikning ikkita asosiy tushuchalari |

№135 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| «Yangi axborot tizimini tatbiq etish» hujjati kim tomonidan ishlab chiqiladi? |
| Xavfsizlik masalalari bilan shugʻullanuvchi boʻlim tomonidan |
| Tashkilot rahbari tomonidan |
| Kadrlar boʻlimi tomonidan |

|  |
| --- |
| Xavfsizlik xodimi |

№136 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdidlarni yuzaga kelish sabablariga koʻra :? |
| Ehtimoliy tahdid,-ehtimol boʻlmagan tahdid. |
| Ehtimoli boʻlgan tahdidlar ,-tabiiy ofatlar |
| Qasddan qilingan tahdidlar. |
| Ichki tahdidlar |

№137 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Axborotning tarqalishi – bu ..... | | | | | | |
| Bu aloqa kanallari va fizik makon orqali barcha sabablarga koʻra, shu  jumladan tutib olish va qayta yoʻnaltirish uchun tarqalganda yoʻqolishi | | | | | | |
| Texnik vositalar yordamida maʻlumot olishning noqonuniy usuli | | | | | | |
| Ilovalar va xizmatlar tomonidan ularning ishlariga taalluqli voqealarni yozish  uchun ishlatiladi. | | | | | | |
| Maʻlumotlarning tarqalishi,  oʻrnatishni oʻz ichiga oladi | uni | tarqatish | yoʻlida | turli | xil | qurilmalarni |

№138 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tahdid nima ? |
| maʻnaviy yoki moddiy zarar yetkazadigan potentsial yoki haqiqiy harakat. |
| texnik vositalar bilan ishlov berilganda axborotning asosiy sifat xususiyatlari  (xususiyatlari) ni buzish salohiyati: |
| jinoiy maqsadlar uchun axborotni axborot tarkibi va mazmunining qisman  yoki sezilarli oʻzgarishi sifatida oʻzgartirish; |
| bevosita moddiy zarar yetkazish maqsadida axborotni yoʻq qilish (yoʻq  qilish). |

№139 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| … - parol, shaxsiy identifikatsiya kodi PIN (Personal Identification Number) hamda “soʻrov javob” xilidagi protokollarda namoyish etiluvchi maxfiy va  ochiq kalitlarni koʻrsatish. |
| biror narsani bilish  asosida |
| biror narsaga egaligi asosida |
| qandaydir daxlsiz xarakteristikalar asosida. |
| biror narsaga egaligi asosida va  biror narsani bilish asosida |

№140 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Maxfiy axborotni oshkor qilmaslik toʻgʻrisidagi majburiyat nimada aks  etgan? |
| Ish beruvchining maxfiy maʻlumotlardan foydalanishga nisbatan oʻz  huquqlarini cheklashga rozi boʻlgan huquqiy hujjatda |
| Uz.Res. ning fuqarolik kodeksida |
| Xodimning ishga qabul qilinganligi toʻgʻrisidagi boʻyruqda |
| Xodim va ish beruvchi oʻrtasida tuzilgan kelishuv shartnomasida |

№141 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Xizmat qilishdan voz kechish hujumidan himoyalanishning eng samarali  yoʻllarini koʻrsating? |
| Tarmoqlararo ekranlar texnologiyasi (Firewall); ipsec protokoli. |
| Tarmoqlararo ekranlar texnologiyasi (Firewall); UDP protokoli. |
| Tarmoqlararo ekranlar texnologiyasi (Firewall); FTP protokoli. |
| Tarmoqlararo ekranlar texnologiyasi (Firewall); mtpro, UDP, ipsec protokoli. |

№142 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tarmoq hujumning bu turi xizmat qilishdan voz kechish hujumi deb  nomlanadi. |
| DOS (Denial-of-service) |
| DOS (Denial-of-system) |
| DOS (system-of-service) |
| DOS (system-of-sabsa) |

№143 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Tarmoq orqali maʻlumot almashish mobaynida yuborilayotgan axborotni  eshitish va oʻzgartirishga qarshi bir necha samarali natija beruvchi texnologiyalar mavjud: |
| IPSec (Internet protocol security) protokoli; VPN (Virtual Private Network)  virtual xususiy tarmoq;IDS (Intrusion Detection System) ruxsatsiz kirishlarni aniqlash tizimi. |
| IPSec (Internet protocol security) protokoli; UDP; IDS (Intrusion Detection  System) ruxsatsiz kirishlarni aniqlash tizimi. |
| IPSec (Internet protocol security) protokoli; VPN (Virtual Private Network) virtual xususiy tarmoq;IDS (Intrusion Detection System) ruxsatli kirishlarni aniqlash tizimi. |
| Obʻekt dasturiy taʻminotiga aygʻoqchilar tomonidan atayin kiritiluvchi turli  xil xatoliklar |

№144 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Ipsec (Internet protocol security) qanday vazifani bajaradi? |

|  |
| --- |
| Bu xavfsizlik protokollari hamda shifrlash algoritmlaridan foydalangan holda  tarmoq orqali xavfsiz maʻlumot almashish imkonini beradi |
| Modul arifmetikasidagi murakkab boʻlmagan amallarning bajarilishi  zaruriyatini koʻrsatish mumkin. Bu oʻz navbatida aytarlicha hisoblash resurslarini talab qiladi |
| Koʻpayish, dasturlarda oʻrnashish, aloqa liniyalari, maʻlumotlarni uzatish tarmoqlari boʻyicha uzatilish, boshqarish tizimlarni ishdan chiqarish va shunga  oʻxshash qobiliyatlarga ega |
| Obʻekt dasturiy taʻminotiga aygʻoqchilar tomonidan atayin kiritiluvchi turli  xil xatoliklar |

№145 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| SSL/TLS protokollari nima uchun yaratilgan |
| Himoyalangan ulanishlar protokoli – Secure Sockets Layer (SSL) Internet  brauzerlarining xavfsizligi muammosini yechish uchun yaratilgan. |
| Bu xavfsizlik protokollari hamda shifrlash algoritmlaridan foydalangan holda  tarmoq orqali xavfsiz maʻlumot almashish imkonini beradi |
| Himoyalangan ulanishlar protokoli – Secure system Layer (SSL) Internet  brauzerlarining xavfsizligi muammosini yechish uchun yaratilgan. |
| Koʻpayish, dasturlarda oʻrnashish, aloqa liniyalari, maʻlumotlarni uzatish  tarmoqlari boʻyicha uzatilish, boshqarish tizimlarni ishdan chiqarish va shunga oʻxshash qobiliyatlarga ega |

№146 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| SSH protokoli. Secure Shell protokoli, SSL/TLSkabi kommunikatsiyalarni  himoyalash uchun qaysi yili yaratilgan |
| 1995 |
| 1996 |
| 1997 |
| 1998 |

№147 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Mafiaboy taxallusi bilan tanilgan mashhur xaker? |
| Maykl kals |
| Jonatan jeyms |
| Maykl jons |
| Jonatoan jons |

№148 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Kiberxavfsizlik inson omilini strategiyalari? |

|  |
| --- |
| Kiber-ishchi kuchini rivojlantirish, Manfaatlar, etakchilik va Ishtirok, Taʻlim  va xabardorlik |
| Bu xavfsizlik protokollari hamda Kiber-ishchi kuchini rivojlantirish,  Manfaatlar, etakchilik va Ishtirok, Taʻlim va xabardorlik |
| Bu xavfsizlik protokollari hamda shifrlash algoritmlaridan foydalangan holda  tarmoq orqali xavfsiz maʻlumot almashish imkonini beradi |
| Himoyalangan ulanishlar protokoli – Secure system Layer (SSL) Internet  brauzerlarining xavfsizligi muammosini yechish uchun yaratilgan. |

№149 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| IT xavfsizligidagi ish faoliyatida asosiy inson omili? |
| Masʻuliyatli va Masʻuliyatsiz |
| biror narsaga egaligi asosida |
| qandaydir daxlsiz xarakteristikalar asosida. |
| biror narsaga egaligi asosida va  biror narsani bilish asosida |

№150 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Kiberxavfsizlikda inson xavfsizligi modeli? |
| Kuzatish, taʻsir qilish, takomillashtirish |
| Kuzatmaslik, taʻsir qilish, takomillashtirish |
| Kuzatish, takomillashtirish |
| Barcha jaavob notoʻgʻri |

№151 Fan bobi– 1; Boʻlimi – 3; Qiyinchilik darajasi– 1;

|  |
| --- |
| Hodisalarni (voqea) yozib borish |
| bu dasturlar va operatsion tizimning muhim dasturiy tadbirlari toʻgʻrisidagi  maʻlumotlarni yozib olish hamda markazlashtirish uchun standart usul. |
| Tarmogining zaif elementlari taxlil- lanadi, takdidlar anikdanadi va  bakolanadi, himoyaning optimal vositalari tanlanadi |
| Xavfsizlik siyosatini amalga oshirish moliyaviy xarajatlarni kisoblash va  masalalarni yechish uchun mos vositalarni tanlash bilan boshlanadi |
| Utkaziladigan tadbirlar niyati buzuk odamlarning tarmokka bostirib kirishini doimo nazorat kilib turishni, axborot obʻektini himoyalash tizimidagi “rakna”larni anikdashni, konfidentsial maʻlumotlardan ruxsatsiz foydalanish  kollarini kisobga olishni talab etadi |

№152 Fan bobi– 1; Boʻlimi – 3; Qiyinchilik darajasi– 1;

|  |
| --- |
| …. - Kiber xavfsizlik xavfini baholash kiber hujum taʻsir qilishi mumkin  boʻlgan axborot aktivlarini aniqlaydi? |
| Kiber tahdidlarni baholash |

|  |
| --- |
| Kiber tahdidlarni boshqarish |
| Kiber tahdidlarni tartiblash |
| Kiber tahdidlarni yuq qilish |

№153 Fan bobi– 1; Boʻlimi – 3; Qiyinchilik darajasi– 1;

|  |
| --- |
| Tahdidlarni baholash |
| Bu potentsial tahdidning ishonchliligi va jiddiyligini,  shuningdek tahdidning haqiqatga aylanish ehtimolini aniqlash amaliyoti |
| Dasturlarning yoki apparat vositalarining moslashuvi kabi texnik  muammolarni, boshqarish vositalarini tanlash vaqtida hisobga olib, oson chetlab oʻtish |
| Rezerv nusxani yaratgan holda,kuniga 24soat, haftasiga 7 kun ishlash  zarurligi |
| Ishlab chiqarish maydonlarining mavjudligi, ekstremal iqlim sharoitlari, oʻrab  turgan tabiiy muhit va shahar muhiti kabi atrof-muhit omillari boshqarish vositalarini tanlashga taʻsir etishi |

№154 Fan bobi– 1; Boʻlimi – 3; Qiyinchilik darajasi– 1;

|  |
| --- |
| Tahdidlarni modellashtirishning nechta asosiy bosqichi mavjud:? |
| 5 |
| 4 |
| 3 |
| 2 |

№155 Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| Xostni baholash-bu? |
| tanqidiy serverlarni baholash |
| maʻlumotlarni tartiblash |
| boshqarish tizimini |
| Dalolatnoma |

№156 Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| ISO 27002 standarti nima? |
| Axborot xavfsizligini boshqarish tizimini ishlab chiqish, joriy etish, uning ishlashi, monitoringi, tahlili, unga xizmat koʻrsatish va uni takomillashtirish  modeli va talablaridan iborat boʻlgan standart |
| Risklarni baxolovchi standart |
| Simsiz tarmoq standarti |
| Protokollar standarti |

№157 Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| «Xodimlarni tanlash va ular bilan ishlashda axborot xavfsizligi» hujjati nima  ? |
| Tashkilotda xodimlarni tanlashda va ular bilan ishlashda axborot xavfsizligini  taʻminlash chora-tadbirlarini aniqlash uchun moʻljallangan |
| Tashkilotda yangi axborot tizimini tatbiq etish jarayonlarini beligilab oʻtish  uchun moʻljallangan |
| axborot xavfsizligining maqsad va prinsiplarini aniqlash uchun moʻljallangan  bulib,oʻz navbatida axborot xavfsizligi obyektlari roʻyxati koʻrsatib oʻtiladi |
| Barcha javoblar toʻgʻri |

№158 Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| «Xodimlarni tanlash va ular bilan ishlashda axborot xavfsizligi» hujjati kim  tomonidan ishlab chiqiladi? |
| xavfsizlik masalalari bilan shugʻullanuvchi boʻlim tomonidan |
| Tashkilot rahbari tomonidan |
| Kadrlar boʻlimi tomonidan |
| Xavfsizlik xodimi |

№159 Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| «Xodimlarni tanlash va ular bilan ishlashda axborot xavfsizligi» hujjati  qancha muddatda yangilanadi? |
| Zaruriyatdan kelib chiqqan holda |
| 1 йил |
| Xodimlar oʻzgarganda |
| 6 oy |

№160 Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| Axborot xavfsizligining asosiy xarakteristirflari nimalar? |
| Konfidentsiallik, butunlik, foydalana olishlik |
| Konfidentsiallik, aniqlik |
| Sirlilik, butunlik, foydalana olishlikni urganib chiqish |
| Identifikatsiya va autentifikatsiya |

№161 Fan bobi– 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| Xavfsizlikka tahdid qaysi sinfga bolinadi? |
| Uyushtirilgan va Tasodifiy tahdid |
| Oldindan oʻylangan va oldindan oʻylanmagan tahdid |
| Uyushtirilmagan va uyushtirilgan tahdid |

|  |
| --- |
| Uyushtirilgan va Tasodifiy tahdid |

№162 Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| Fizik va texnik himoyalash vositalarining funksiyasi nima? |
| Tashkiliy meyorlar kamchiligini bartaraf etish |
| Foydalanuchilarning tizim resurslariga kirish qoidalarini ishlab chiqish |
| Kirishni cheklab qoʻyish |
| Yashirin holdagi buzgʻinchilarni ushlab turuvchi omil |

№163 Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| ... - josuslik, buzgʻunchilik, sabotaj, suiqasd va hujumlarini amalga oshirishi mumkin boʻlgan xorijiy razvedka tashkilotlari va terrorchilar qaysi darajaliga kiradi. |
| 1-darajali tahdid |
| 5-darajali tahdid |
| 3-darajali tahdid |
| 4-darajali tahdid |

№164 Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| Parol-bu: |
| Foydalanuvchi hamda uning axborot almashinuvidagi sherigi biladigan  axborot |
| Foydalanuvchining nomi |
| Axborotni shifrlash kaliti hamda uning axborot almashinuvidagi sherigi  biladigan axborot |
| Axborotni tashish vositasi |

№165 Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi – 1;

|  |
| --- |
| IDS (Intrusion Detection System)nima ? |
| ruxsatsiz kirishlarni aniqlash tizimi |
| ruxsatsiz kirishlarni boshqarish tizimi |
| ruxsatsiz kirishlarni toʻxtatish tizimi |
| ruxsatsiz kirishlarni bogʻlash |

Fan bobi – 1; Boʻlimi – 3; Qiyinchilik darajasi– 1;

|  |
| --- |
| “Xavfsizlik siyosati” deb ataluvchi korporativ kompьyuter tarmoqlarini sanab  oʻting |

|  |
| --- |
| umumiy printsiplar va ishlashning muayyan koidalari |
| foydalanish reglamenti xamda tarmokdan foydalanuvchilar |
| obʻektlar, resurslar va muolajalarni bevosita ximoyasi |
| Toʻgʻri javob yoʻq |

№167 Fan bobi– 1; Boʻlimi – 3; Qiyinchilik darajasi– 1;

|  |
| --- |
| Himoya tizimini loyihalash va amalga oshirish bosqichlarini koʻrsating? |
| xavf-xatarni taxlillash, xavfsizlik siyosatini amalga oshirish, xavfsizlik  siyosatini madadlash |
| foydalanishlarni taxlillash, xavfsizlik xodimlarini tanlash, tarmoqni qayta  loyihalash |
| tizim kamchiligini izlash, xavfsizlik xodimlarinitanlash, siyosatni qayta  koʻrish |
| dasturlarni yangilash, xavfsizlik xodimlarinitanlash, tarmoqni qayta  loyihalashni tahlil qilib chiqish |

№168 Fan bobi – 3; Boʻlimi – 1; Qiyinchilik darajasi – 2;

|  |
| --- |
| Fоydalanuvchining tarmоqdagi harakatlarini va resurslardan fоydalanishga  urinishini qayd etish-bu: |
| Ma`murlash |
| Autentifikatsiya |
| Identifikatsiya |
| Sertifikatsiyalash |

№169 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| Foydalanuvchini uning identifikatori (nomi) boʻyicha aniqlash jarayoni-bu: |
| Identifikatsiya |
| Autentifikatsiya |
| Avtorizatsiya |
| Maʻmurlash (accounting) |

№170 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Foydalanuvchini autentifikatsiyalashda qanday maʻlumotdan foydalaniladi? |
| Parol |
| Ismi va ID raqami |
| ERI algoritmlari |
| Telefon raqami |

№171Fan bobi – 3; Boʻlimi – 1; Qiyinchilik darajasi – 2;

|  |
| --- |
| Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar  axborotdan foydalana olishliklari-bu: |
| Foydalanuvchanligi |
| Maʻlumotlar butunligi |
| Axborotning konfedensialligi |
| Ixchamligi |

№172 Fan bobi – 4; Boʻlimi – 2; Qiyinchilik darajasi – 1;

|  |
| --- |
| Eng koʻp axborot xavfsizligini buzilish holati-bu: |
| Tarmoqda ruxsatsiz ichki foydalanish |
| Tizimni loyihalash xatolaridan foydalanish |
| Tashqi tarmoq resursiga ulanish |
| Simsiz tarmoqqa ulanish |

№173 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Dinamik parol-bu: |
| Bir marta ishlatiladigan parol |
| Koʻp marta ishlatiladigan parol |
| Foydalanuvchi ismi va familiyasining nomi |
| Sertifikat raqamlari |

№174 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Bugungi kunga kelib baʻzi bir davlatlarning rahbarlari qanday dasturlarni  yaratishni moliyalashtirmoqdalar? |
| Kiber dasturlarni |
| Windows dasturlarni |
| Ishonchli dasturlarni |
| Yangi dasturlarni |

№175 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axbоrоt tizimlari xavfsizligining auditi-bu? |
| Axborot tizimlarining himoyalanishining joriy holati, tizim haqida obʻyektiv  maʻlumotlarni olish va baholash |
| Ma`lumоtlarini tahlillash va chоra koʻrishni tizim haqida subyektiv  maʻlumotlarni olish va baholashni tahlil qiladi |
| Ma`lumоtlarini tarqatish va boshqarish |
| Axbоrоtni yigʻish va korxona tarmogʻini tahlillash |

№176 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axbоrоt infratuzilmasi-bu: |
| Servislarni taʻminlovchi vositalar, aloqa liniyalari, muolajar, meʻyoriy  xujjatlar |
| Kоmpyuterlardan foydalanivchilar uchun xizmatlarni koʻpaytirish uchun  muolajar, meʻyoriy hujjatlar |
| Axbоrоt tizimlarini baholash va tizimni boshqarish |
| Kоmpyuter tizimlarini nazoratlash, aloqa liniyalarini tekshirish |

№177 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborotni ximoyalash konsepsiyasi–bu: |
| Axborot xavfsizligi muammosiga rasmiy qabul qilingan qarashlar tizimi va  uni zamonaviy tendensiyalarni hisobgaolgan holda yechish yoʻllari |
| Axborotga boʻlgan hujumlar majmui |
| Axborotga boʻlgan foydalanishlar majmui |
| Axborotni yaratish, qayta ishlashga boʻlgan qarashlar va uni zamonaviy  tendensiyalarni hisobgaolgan holda yechish yoʻllarini inobatga olgan holati |

№178 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborotning buzilishi yoki yoʻqotilishi xavfiga olib keluvchi himoyalanuvchi  obʻektga qarshi qilingan xarakatlar kanday nomlanadi? |
| Tahdid |
| Zaiflik |
| Hujum |
| Butunlik |

№179 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborotni qanday taʻsirlardan himoyalash kerak? |
| Axborotdan ruxsatsiz foydalanishdan, uni buzilishdan yoki yoʻq qilinishidan |
| Axborotdan qonuniy foydalanishdan, uni qayta ishlash yoki sotishdan |
| Axborotdan qonuniy foydalanishdan, uni qayta ishlash yoki foydalanishdan  oʻrganishi |
| Axborotdan tegishli foydalanishdan, uni tarmoqda uzatishdan |

№180 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborotni ishonchli himoya mexanizmini yaratishda quydagilardan qaysi biri  muhim hisoblanadi? |
| Tashkiliy tadbirlar |
| Ommaviy tadbirlar |

|  |
| --- |
| Antivirus dasturlari |
| Foydalanuvchilar malakasi |

№181 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborotni himoyalash tizimida bajarilishi shart boʻlgan qoidalar  yoʻriqnomalar va qoʻllanmalar majmuyi–bu: |
| Axborot xavfsizligining huquqiy taʻminoti |
| Axborot xavfsizligining tashkiliy taʻminoti |
| Axborot xavfsizligining uslubiy taʻminoti |
| Axborot xavfsizligining amaliy taʻminoti |

№182 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborotdan qanday foydalanish ruxsat etilmagan deb yuritiladi? |
| Foydalanishga oʻrnatilgan chegaralash qoidalarini buzadigan |
| Axborot butunligini buzmaydigan |
| Axborot konfidensialligini buzmaydigan |
| Foydalanishga oʻrnatilgan chegaralash qoidalarini buzmaydigan |

№183 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot xavfsizligi konsepsiyasini ishlab chiqish necha bosqichdan iborat? |
| 3 bosqich |
| 4 bosqich |
| 5 bosqich |
| 6 bosqich |

№184 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot xavfsizligi konsepsiyasini ishlab chiqishning birinchi bosqichida  nima qilinadi? |
| Himoyalanuvchi obyektning qiymati aniqlanadi |
| Buzgʻunchining boʻlishi mumkin boʻlgan harakatlari taxlillanadi |
| Axborotni himoyalash vositalarining ishonchliligi baholanadi |
| Tizimni loyihalash jadallashtiriladi |

№185 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot xavfsizligi konsepsiyasini ishlab chiqishning ikkinchi bosqichida  nima qilinadi? |
| Buzgʻunchining boʻlishi mumkin boʻlgan harakatlari taxlillanadi |
| Tizimni loyihalash jadallashtiriladi |

|  |
| --- |
| Himoyalanuvchi obyektning qiymati aniqlanadi |
| Axborotni himoyalash vositalarining ishonchliligi baholanadi va urganiladi |

№186 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot xavfsizligi konsepsiyasini ishlab chiqishning uchunchi bosqichida  nima qilinadi? |
| Obyektga oʻrnatilgan axborotni himoyalash vositalarining ishonchliligi  baholanadi |
| Loyihalash jadallashtiriladi |
| Buzgʻunchining boʻlishi mumkin boʻlgan harakatlari taxlillanadi va  ishonchliligi baholanadi |
| Himoyalanuvchi obyektning qiymati aniqlanadi |

№187 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot xavfsizligining huquqiy taʻminotiga nimalar kiradi? |
| Qonunlar, aktlar, meʻyoriy-huquqiy hujjatlar, qoidalar, yoʻriqnomalar,  qoʻllanmalar majmui |
| Qoidalar yoʻriqnomalar, tizim arxetikturasi, xodimlar malakasi, yangi  qoidalar, yangi yoʻriqnomalar, qoʻllanmalar majmui |
| Qoidalar, yoʻriqnomalar, tizim strukturasi, dasturiy taʻminot |
| Himoya tizimini loyihalash, nazorat usullari |

№188 Fan bobi – 4; Boʻlimi – 3; Qiyinchilik darajasi – 3;

|  |
| --- |
| Axborot xavfsizligining huquqiy taʻminoti qaysi meʻyorlarni oʻz ichiga oladi? |
| Xalqaro va milliy huquqiy meʻyorlarni |
| Tashkiliy va xalqaro meʻyorlarni |
| Ananaviy va korporativ meʻyorlarni |
| Davlat va nodavlat tashkilotlari meʻyorlarni |

№189 Fan bobi– 4; Boʻlimi – 3; Qiyinchilik darajasi– 3;

|  |
| --- |
| Axborot xavfsizligini taʻminlovchi choralarni koʻrsating? |
| Huquqiy, tashkiliy-maʻmuriy, injener-texnik |
| Axloqiy, tashkiliy-maʻmuriy, fizikaviy-kimyoviy |
| Dasturiy, tashkiliy-maʻmuriy, huquqiy |
| Apparat, texnikaviy, huquqiy |

№190 Fan bobi– 4; Boʻlimi – 3; Qiyinchilik darajasi– 3;

|  |
| --- |
| Anomaliyani aniqlashda uchta 3 asosiy yondashuv qanday? |

|  |
| --- |
| Nazoratli, Nazoratsiz, Yarim nazorat ostida |
| Nazoratli, Nazoratsiz, |
| Nazoratsiz, Yarim nazorat ostida |
| Nazoratli, Nazoratsiz, Yarim nazorat ostida |

№191 Fan bobi– 4; Boʻlimi – 3; Qiyinchilik darajasi– 3;

|  |
| --- |
| Korxona xavfsizlik xizmatining asosiy vazifalari? |
| Korxona xavfsizligini taʻminlash |
| Ishl Xodimlarni nazorat qilish |
| Mahsulot sifatini tekshirish |
| Toʻgʻri javob yoʻq |

№192 Fan bobi - 4; Boʻlimi - 3; Kiyinchilik darajasi - 3;

|  |
| --- |
| Axborot xavfsizligini buzuvchilarni qanday kategoriyalarga ajratish mumkin? |
| Sarguzasht qidiruvchilar, gʻoyaviy xakerlar, xakerlar-professionallar,  ishonchsiz xodimlar |
| Buzgunchilar, gʻoyaviy xakerlar, xakerlar-professionallar, sotqinlar,  krakerlar va ularning guruhlari |
| Buzgunchilar, dasturchilar, xakerlar, sotqinlar |
| Foydalanuvchilar, xodimlar, xakerlar, sotqinlar |

№193 Fan bobi– 4; Boʻlimi – 3; Qiyinchilik darajasi– 3;

|  |
| --- |
| Axborot xavfsizligi strategiyasi va himoya tizimi arxitekturasi nima asosida  ishlab chiqiladi? |
| Axborot xavfsizligi konsepsiyasi asosida |
| Tizimni loyihalashda yuzaga keladigan vaziyat asosida |
| Axborot tizimi qurilmalarini soddalashtirish asosida |
| Himoyani buzishga boʻlgan urinishlar asosida |

№194 Fan bobi– 4; Boʻlimi – 3; Qiyinchilik darajasi– 3;

|  |
| --- |
| Axborot xavfsizligi siyosatini ishlab chiqishda avvalo nimalar aniqlanadi? |
| Himoya qilinuvchi obyekt va uning vazifalari |
| Mavjud himoya vositalari |
| Himoya tizimiga talablar |
| Himoya tizimini tashkil etish muddati va vazifasi |

№195 Fan bobi– 4; Boʻlimi – 3; Qiyinchilik darajasi– 3;

… - bu standart boʻlishi mumkin boʻlmagan hodisalar qatoriga

|  |
| --- |
| qoʻshilmaydigan hamda xizmat holatini uzib qoʻyish yoki xizmat sifati  yomonlashishi holatlariga olib keladigan har qanday hodisaga aytiladi |
| Insident (mojoro, hodisa) -? |
| Axborotni himoyalash |
| Xavfsizlikni amalga oshirish vaqti meьyorlari |
| Axborotni himoyalash bosqichlari |

№196 Fan bobi– 4; Boʻlimi – 3; Qiyinchilik darajasi– 3;

|  |
| --- |
| Axborot xavfsizligi strategiyasi va himoya tizimi arxitekturasi nima asosida  ishlab chiqiladi? |
| Axborot xavfsizligi konsepsiyasi |
| Standartlar va xalqaro standartlar markazi |
| Farmonlar |
| Buyruqlar |

№197 Fan bobi– 4; Boʻlimi – 3; Qiyinchilik darajasi– 3;

|  |
| --- |
| Avtorizatsiya tizimdan foydalanishda qanday vakolat berani? |
| Subyektning harakat doirasi va foydalanadigan resurslarni belgilaydi |
| Resurslardan foydalanishga imkon beradi va obyekni toʻgʻri ishlashini  nazorat beradi |
| Resurslarni oʻzgartirishga imkon beradi |
| Subyektni foydalanishi taqiqlangan resurslarni belgilaydi |

№198 Fan bobi– 4; Boʻlimi – 3; Qiyinchilik darajasi– 3;

|  |
| --- |
| Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taʻminlashning  zaruriy sharti–bu: |
| Tamoqlararo ekranlarning oʻrnatilishi |
| Tashkiliy ishlarni bajarilishi |
| Globol tarmoqdan uzib qoʻyish |
| Aloqa kanallarida optik toladan foydalanish |

№199 Fan bobi– 4; Boʻlimi – 2; Qiyinchilik darajasi– 1;

|  |
| --- |
| Agar axborotning oʻgʻirlanishi moddiy va maʻnaviy boyliklarning yoʻqotilishi bilan bogʻliq boʻlsa bu nima deb yuritiladi? |
| Jinoyat sifatida baholanadi |
| Ragʻbat hisoblanadi |
| Buzgunchilik hisoblanadi |
| Guruhlar kurashi hisoblanadi |

№200 Fan bobi– 4; Boʻlimi – 3; Qiyinchilik darajasi– 3;

|  |
| --- |
| Maʻlumotlarni oʻqib olishni qiyinlashtirish maqsadida ularni kriptografiya  usullari orqali kodlashga nima deyiladi? |
| Niqoblash usuli |
| Toʻsqinlik usuli |
| Majburlash usuli |
| Kriptografiya usuli |