|  |
| --- |
| **№ 1** |
| |  | | --- | | Risk ta‘rifi to‘g‘ri keltirilgan qatorni belgilang. | | noaniqlikning maqsadlarga ta'siri |   **№ 2.** |
| |  | | --- | | …. bu xavfsizlik tizimining kamchiligi bo‘lib, xavfni ro'yobga chiqarishga imkon beradi. Bu tushuncha quyidagilardan qay biriga tegishli? | | Zaiflik |   **№ 3.** |
| |  | | --- | | Axborot xavfsizligi xavflarini (risk) boshqarishga kirish fani maqsadiga zid bo’lgan qatorni belgilang. | | Faqat risklarni aniqlash va hisoblash |   **№ 4.** |
| |  | | --- | | Risklarni boshqarishda xavfsizlik siyosatining eng asosiy vazifalaridan biri bu nima? | | Himoya tizimida potensial xavfli nuqtalarni qidirib topish va ularni bartaraf etish |   **№ 5.** |
| |  | | --- | | Axborot xavf xatarlari nuqtai nazaridan “noaniqlik” nimani anglatadi? | | Ma'lumotlarning yetishmasligi (hatto qisman) |   **№ 6.** |
| |  | | --- | | Axborot xavf xatarlari nuqtai nazaridan “Hodisa”ga bog‘liq bo‘lmagan tushunchani belgilang. | | Ijtimoiy himoyalanish |   **№ 7.** |
| |  | | --- | | Standart operatsiyalar qatoriga qo‘shilmaydigan hamda xizmat holatini uzib qo‘yish yoki xizmat sifati yomonlashishi holatlariga olib keladigan har qanday hodisa bu nima? | | Insident |   **№ 8.** |
| |  | | --- | | Zaiflik tushunchasi to’g’ri ko’rsatilgan qatorni belgilang? | | Xavfsizlik tizimining kamchiligi, bu xavfni ro'yobga chiqarishga imkon beradi |   **№ 9.** |
| |  | | --- | | Aktiv tushunchasi to’g’ri ko’rsatilgan qatorni belgilang. | | Tashkilot uchun eng qimmatli narsalar |   **№ 10.** |
| |  | | --- | | Boshqarish tushunchasi to’g’ri ko’rsatilgan qatorni belgilang. | | Xavfni o'zgartirish chorasi |   **№ 11.** |
| |  | | --- | | Risklarni boshqarish vositalarini belgilang. | | Riskni o'zgartirishga qaratilgan har qanday jarayonlar, siyosatlar, qurilmalar, protseduralar |   **№ 12.** |
| |  | | --- | | Rikslar menejmenti nima? | | Risk sohasidagi tashkilotni boshqarish va boshqarishning muvofiqlashtirilgan faoliyati |   **№ 13.** |
| |  | | --- | | Axborot xavfsizligi xavfini boshqarish jarayoni tashkil etuvchilari to’liq ko’rsatilgan qatorni belgilang. | | kontekstni aniqlash, riskni baholash, davolash, qabul qilish, ma'lumot almashish, monitoring |   **№ 14.** |
| |  | | --- | | Xavfni qayta ishlash samaradorligi nimaga bog’liq? | | xavfni baholash natijalariga |   **№ 15.** |
| |  | | --- | | Xavfli hodisaning yo'lini sababdan oqibatgacha tavsiflash va tahlil qilishning sxematik usulini belgilang. | | “galstuk-babochka” tahlil usuli |   **№ 16.** |
| |  | | --- | | Hodisa sabablarini nosozlik daraxti yordamida o'rganishni va voqealar daraxti yordamida oqibatlarini tahlil qilishni birlashtiruvchi tahlil usulini belgilang. | | “galstuk-babochka” tahlil usuli |   **№ 17.** |
| |  | | --- | | Asosiy yo'nalishi sabablar va xavfli hodisalar oqibatlari o'rtasidagi to'siqlarga qaratilgan tahlil usulini belgilang. | | “galstuk-babochka” tahlil usuli |   **№ 18.** |
| |  | | --- | | Guruh ishiga malakali mutaxassislarni jalb qilish, tizimli tahlildan foydalanish, barcha mumkin bo'lgan taxminlar va farazlarni ko'rib chiqish, natijalarni tushunarli shaklda grafik tarzda ko'rsatish, qo'shimcha ma'lumot talab qilinadigan joylarni aniqlash, ijobiy va salbiy natijalarga olib keluvchi omillarni aniqlash imkoniyati kabi afzalliklar qaysi tahlil usuliga tegishli? | | “galstuk-babochka” tahlil usuli |   **№ 19.** |
| |  | | --- | | Bir vaqtning o'zida bir nechta voqealar sodir bo'lishi mumkin bo'lgan, tekshirilayotgan yakuniy voqea va vaziyatlarning vujudga kelish yo'llarini vizual ravishda taqdim etuvchi tahlil usulini belgilang. | | “Nosozlik daraxti” tahlil usuli |   **№ 20.** |
| |  | | --- | | Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. | | “VA” mantiqiy elementi |   **№ 21.** |
| |  | | --- | | Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. | | “YOKI” mantiqiy elementi |   **№ 22.** |
| |  | | --- | | Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. | | Asosiy hodisa-tahlilni davom ettirishdan mantiq yo‘q |   **№ 23.** |
| |  | | --- | | Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. | | Hodisa tahlil qilinmaydi |   **№ 24.** |
| |  | | --- | | Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. | | Tahlil qilinishi kerak bo’lgan hodida |   **№ 25.** |
| |  | | --- | | Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. | | O‘tkazish-hodisa tahlilini boshqa sahifa yoki joyda davom ettirish |   **№ 26.** |
| |  | | --- | | Axborot xavfsizligi risklarini boshqarish uchun zarur bo'lgan asosiy mezonlar, ko'lam va chegaralarni aniqlash, axborot xavfsizligi risklarini boshqarishni amalga oshirish uchun tegishli tuzilmani tuzishni ifodalovchi tushunchani belgilang. | | kontekstni o’rnatish |   **№ 27.** |
| |  | | --- | | Kontekst turlarini belgilang. | | Ichki kontekst, Tashqi kontekst |   **№ 28.** |
| |  | | --- | | Tashqi kontekst to’g’ri keltirilgan qatorni belgilang. | | Tashkilot o'z maqsadlariga erishmoqchi bo'lgan tashqi muhit |   **№ 29.** |
| |  | | --- | | Ichki kontekst to’g’ri keltirilgan qatorni belgilang. | | Tashkilot o'z maqsadlariga erishishga undaydigan ichki muhit |   **№ 30.** |
| |  | | --- | | Madaniy, ijtimoiy, huquqiy, moliyaviy, texnologik, iqtisodiy, xalqaro, mintaqaviy, milliy yoki mahalliy darajadagi tabiiy va bozor muhiti, tashkilot maqsadlariga ta'sir qiluvchi asosiy omillar va tendentsiyalar, manfaatdor tomonlar munosabatlari, anglashuv va qiymatlilik qaysi kontekst turiga tegishli? | | Tashqi kontekst |   **№ 31.** |
| |  | | --- | | Yetakchilik, tashkiliy tuzilma, vazifalar va mas'uliyat, siyosatlar, maqsadlar va ularga erishish strategiyalari, resurslar va bilimlarga nisbatan, axborot tizimlari, axborot oqimi va qaror qabul qilish jarayonlari, ichki manfaatdor tomonlar bilan munosabatlar, ularning o'zaro anglashuv va qiymatlilik, tashkilot madaniyati, qabul qilingan standartlar, ko'rsatmalar va modellar, shartnoma munosabatlarining shakli va ko'lami qaysi kontekst turiga tegishli? | | Ichki kontekst |   **№ 32.** |
| |  | | --- | | Risklarni boshqarish maqsadiga zid bo’lgan qatorni belgilang. | | identifikatsiya, autentifikatsiya |   **№ 33.** |
| |  | | --- | | Axborot xavfsizligi hodisasi natijasida tashkilotga yetkazilgan zarar yoki zarar darajasini belgilashda ishtirok etmaydigan tushunchani belgilang. | | Tashkiliy choralar |   **№ 34.** |
| |  | | --- | | Riskni qabul qilish mezonlari tuzilishida hisobga olinishi kerak bo’lgan jihatlarni belgilang. | | Biznes mezonlari, huquqiy va tartibga soluvchi jihatlar, Operatsiyalar, Texnologiya, Moliya, Ijtimoiy va gumanitar omillar |   **№ 35.** |
| |  | | --- | | Aktiv namunalari to’g’ri keltirilgan qatorni belgilang. | | Xodimning ish stoli, noutbuk yoki telefoni, serverlar, qurilmalardagi ilovalar, qo'llab-quvvatlash tizimlari |   **№ 36.** |
| |  | | --- | | ISO 27001ni joriy qilishda tashkilotlarning bajarishi kerak bo'lgan birinchi qadam bu -… | | axborot aktivlarini aniqlash |   **№ 37.** |
| |  | | --- | | Axborot aktivlarini ishlab chiqarish, texnik xizmat ko'rsatish, foydalanish va xavfsizligini nazorat qilish uchun mas'ul bo'lgan jismoniy yoki yuridik shaxs kim? | | Aktiv egasi |   **№ 38.** |
| |  | | --- | | Axborot aktivlarining turlarini belgilang. | | Asosiy, yordamchi |   **№ 39.** |
| |  | | --- | | Asosiy axborot aktivlari keltirilgan qatorni belgilang. | | Biznes jarayonlari va faoliyati, axborot |   **№ 40.** |
| |  | | --- | | Yordamchi axborot aktivlari keltirilgan qatorni belgilang. | | Apparat taminot, dasturiy ta'minot, tarmoq, xodimlar, sayt, tashkiliy tuzilma |   **№ 41.** |
| |  | | --- | | Asosiy aktiv “axborot” tarkibiga kirmaydigan qatorni belgilang. | | Qalbakilashtirilgan ma'lumotlar |   **№ 42.** |
| |  | | --- | | Yordamchi aktiv “Apparat ta'minot” tarkibiga kirmaydigan qatorni belgilang. | | To'plash, saqlash, qayta ishlash va uzatish uzoq davom etadigan qimmatli ma'lumotlar |   **№ 43.** |
| |  | | --- | | Yordamchi aktiv “Dasturiy ta'minot” tarkibiga kirmaydigan qatorni belgilang. | | Ma'lumotni qayta ishlash uskunalari |   **№ 44.** |
| |  | | --- | | Yordamchi aktiv “Shaxs” to’g’ri va to’liq keltirilgan qatorni belgilang. | | Qaror qabul qiluvchi, Foydalanuvchilar, Operatsion va texnik xodimlar, Ishlab chiquvchi |   **№ 45.** |
| |  | | --- | | Aktivlarni aniqlashning eng yaxshi usuli bu nima? | | mulk egalari bilan suhbat |   **№ 46.** |
| |  | | --- | | Bu asosiy hodisadan (ETA-Event tree analysis) kelib chiqadigan hodisalar ketma -ketligini tuzish algoritmi. Favqulodda vaziyatning rivojlanishini tahlil qilish uchun ishlatiluvchi usulini belgilang. | | “Voqealar daraxti” tahlil usuli |   **№ 47.** |
| |  | | --- | | Muayyan holatlarning paydo bo'lishi yoki o'zgarishi nima deb ataladi? | | Hodisa |   **№ 48.** |
| |  | | --- | | Hodisa (yoki insident)ning qanday turlari mavjud? | | Normal, Avariyaviy |   **№ 49.** |
| |  | | --- | | Quyidagi ta’rifga mos kalit so’zni belgilang. | | Kontekst dastlab \_\_\_\_\_\_\_\_\_\_\_\_ riskni baholashda o'rnatiladi. | | Yuqori darajali |   **№ 50.** |
| |  | | --- | | Agar kontekst xavfni maqbul darajaga tushirish uchun zarur bo'lgan harakatlarni samarali aniqlash uchun yetarli ma'lumotni taqdim etsa, u holda vazifa tugallangan hisoblanadi va risk ustida qanday harakat amalga oshiriladi? | | riskni qayta ishlash |   **№ 51.** |
| |  | | --- | | Axborot resurslari, ularning turlari, tuzilishi, toifalari, axborot resurslarini boshqarish tamoyillari, axborot tizimlari, ularning turlari, tuzilishi, tasnifi va ularning axborot xavfsizligini ta'minlash usullarini tahlil qilish natijasida nimalar aniqlanadi? | | Korxona aktivlari |   **№ 52.** |
| |  | | --- | | Korxonani nomi, nufuzi va imidji kabilar qimmatli aktivlarni qaysi turiga mansub hisoblanadi? | | Korxonani nomoddiy manbalari |   **№ 53.** |
| |  | | --- | | Korxonadagi kompyuter qurilmalari, telekommunikatsiya va boshqa qurilmalari qimmatli aktivlarni qaysi turiga mansub hisoblanadi? | | Korxonaning moddiy manbalari |   **№ 54.** |
| |  | | --- | | Har bir qimmatli aktivning axborot xavfsizligi buzilgan taqdirda, kompaniya qancha zarar ko'rishini oldindan tahlil qilishda, tashkilotning biznes jarayonlari uchun aktivlarning muhimligini baholashda aktivlarning qiymati nima asosida aniqlanadi? | | Ekspert xulosasi |   **№ 55.** |
| |  | | --- | | … - bu aktivlarning qiymatini korxona yoki tashkilot uchun ahamiyati nuqtai nazaridan baholash va aktivlarni himoya qilishning zarur darajasini aniqlash maqsadida amalga oshiriladi. Nuqtalar o’rniga to’g’ri keladigan bandni ko’rsating | | Aktivlar qiymatini baholash |   **№ 56.** |
| |  | | --- | | Aktivlar qaysi o’lchovlar asosida baholanadi? | | Maxfiylik, yaxlitlik va mavjudlik. |   **№ 57.** |
| |  | | --- | | Sifat darajasiga ko’ra baholashda nechta darajadan foydalanish eng qulay hisoblanadi? | | 5 |   **№ 58.** |
| |  | | --- | | Tashkilotning mumkin bo'lgan zaif tomonlarini sanab o'tish va ularni "kuchliligi" ga qarab toifalarga ajratish qanday jarayon hisoblanadi? | | Zaiflilik tahlili |   **№ 59.** |
| |  | | --- | | Zaifliklar qanday toifalarga ajraladi? | | Texnik, texnologik va tashkiliy |   **№ 60.** |
| |  | | --- | | Loyihalashdagi xatoliklar va ma’muriy xatoliklar zaiflikni qaysi turiga mansub? | | Texnologik |   **№ 61.** |
| |  | | --- | | Mumkin bo'lgan hodisadan keyin tizimni asl holatiga qaytarish xarajatlarini hisobga olgan holda hisoblanadigan yo'qotish nima deb ataladi? | | Zarar |   **№ 62.** |
| |  | | --- | | Axborot xavfsizligi buzilishi natijasida tashkilotga yetkazilgan zararni sifat bo'yicha baholashda baholashning nechta darajasi tavsiya etiladi? | | 3 |   **№ 63.** |
| |  | | --- | | Zararni baholashda nechta me’zondan foydalanish taklif etiladi? | | 4 |   **№ 64.** |
| |  | | --- | | Axborot xavfsizligi buzilishidan kelib chiqadigan moddiy zarar qanday turdagi zarar hisoblanadi? | | to'g'ridan-to'g'ri zarar |   **№ 65.** |
| |  | | --- | | Nufuzga putur yetishi, ishbilarmonlik aloqalarini uzish, tashkilot imidjini yaxshilash uchun qo'shimcha xarajatlar va boshqalar qaysi turdagi zararga kiradi? | | Boshqa turdagi yo'qotishlar |   **№ 66.** |
| |  | | --- | | Axborot xavfsizligiga tahdidlarni amalga oshirish ehtimoli ko'rsatkichi nimalar asosida tuziladi? | | Ekspert baholari, statistik ma'lumotlar asosida yoki o'tgan davrdagi tahdidlar to'g'risidagi hisobotlar |   **№ 67.** |
| |  | | --- | | Qachon tahdidlarni amalga oshirish ehtimoli dargumon deb hisoblanadi? | | Agar tahdidni amalga oshirish uchun ob'ektiv shartlar mavjud bo'lmasa |   **№ 68.** |
| |  | | --- | | Qachon tahdidlarni amalga oshirish ehtimoli past deb hisoblanadi? | | Tahdidning yuzaga kelishi uchun ob'ektiv shartlar mavjud bo'lganda |   **№ 69.** |
| |  | | --- | | Qachon tahdidni amalga oshirish ehtimoli o'rtacha deb hisoblanadi? | | Xavf amalga oshishining ob'ektiv old shartlari mavjud bo'lganda, lekin amalga oshirilayotgan xavfsizlik choralari yetarli bo'lmagan taqdirda |   **№ 70.** |
| |  | | --- | | Qachon tahdidlarni amalga oshirish ehtimoli yuqori deb hisoblanadi? | | Tahdidning yuzaga kelishi uchun ob'ektiv shartlar mavjud bo'lganda va xavfsizlik choralari ko'rilmaganda |   **№ 71.** |
| |  | | --- | | Tahdidning amalga oshirilishi ehtimoli va ushbu tahdid qaratilgan qimmatbaho aktivning dastlabki xavfsizlik darajasini hisobga olgan holda, ma'lum bir tashkilotda muayyan tahdid amalga oshirilishini ko'rsatuvchi bu nima? | | Tahdidning tadbiq ko'rsatkichi |   **№ 72.** |
| |  | | --- | | Zarar va hujum ehtimolini ko’paytmasining natijasi nimani beradi? | | Risk |   **№ 73.** |
| |  | | --- | | Xavfdan qochish uchun biznes usullarini o'zgartiradigan har qanday harakatlar nima deb ataladi? | | Riskdan qochish |   **№ 74.** |
| |  | | --- | | Boshqalarning xavf va zararlar uchun javobgarlikni o'z zimmasiga olishi nima deyiladi? | | Riskni uzatish |   **№ 75.** |
| |  | | --- | | Yo'qotish ehtimoli va hajmini kamaytirish nima deb ataladi? | | Riskni kamaytirish |   **№ 76.** |
| |  | | --- | | Xavfga qarshi choralar natijasida riskning boshlang'ich yoki maqbul qiymatini qabul qilinishiga nima deyiladi? | | Riskni qabul qilish |   **№ 77.** |
| |  | | --- | | Agar xavf juda muhim darajaga ega bo'lsa va uni qisqa vaqt ichida kamaytirish, qabul qilish yoki uzatish mumkin bo'lmasa, unda qanday chora qo'llaniladi? | | Riskni tubdan kamaytirish |   **№ 78.** |
| |  | | --- | | Tashkilotning axborot xavfsizligini ta'minlash darajasini baholashda tashkilotdagi axborot xavfsizligi darajasiga bog'liq bo'lgan nechta parametr hisobga olinadi? | | 3 |   **№ 79.** |
| |  | | --- | | Har qanday qimmatli ma’lumotlar, qurilma yoki tashkilot tizimlarining boshqa komponentalari nima deb ataladi? | | Aktiv |   **№ 80.** |
| |  | | --- | | Qaysi standartda joriy qilishda tashkilotlarning bajarishi kerak bo’lgan birinchi narsa bu axborot aktivini aniqlash deb ko‘rsatilgan? | | ISO 27001 |   **№ 81.** |
| |  | | --- | | Axborot aktivlarini ishlab chiqarish, texnik xizmat ko'rsatish, foydalanish va xavfsizligini nazorat qilish uchun mas'ul bo'lgan jismoniy yoki yuridik shaxs bu kim? | | Aktiv egasi |   **№ 82.** |
| |  | | --- | | Sabablar, oqibatlar, ta'sirlar, xavf zonalari va hodisalar to'g'risida olingan ma'lumotlarga asoslangan xavf-xatar bayonoti nima deb ataladi? | | Oddiy spetsifikatsiya |   **№ 83.** |
| |  | | --- | | …. - bu potentsial xavflar haqidagi ikkita savolga javob: nima uchun biz bu xavflarga duch kelishimiz kerak (yoki bo'lmasligi kerak) va biz ilgari duch kelganmizmi degan savollarga javobdir. | | bazaviy identifikatsiya |   **№ 84.** |
| |  | | --- | | Bu qadam oldingi qadamlarga qaraganda ko'proq vaqt talab qiladi, lekin u xavfni to'g'ri baholash uchun zarur bo'lgan tafsilotlarni beradi. Gap qaysi bosqich haqida bormoqda? | | batafsil identifikatsiya |   **№ 85.** |
| |  | | --- | | Bunda xatarlar ishning tegishli qismlari bilan taqqoslanadi. Gap qaysi jarayon haqida ketmoqda? | | ichki o’zaro tekshiruv |   **№ 86.** |
| |  | | --- | | Dasturiy ta’minot, biznes ilovalar va tarmoq qanday turdagi aktivga kiradi? | | yordamchi |   **№ 87.** |
| |  | | --- | | Insident sababli aktiv(lar) tomonidan ko'rsatiladigan xizmat tiklangunga qadar jarayondagi to'xtalishlar qiymati parametri ta’sirni baholashni qaysi turiga kiradi? | | Bevosita |   **№ 88.** |
| |  | | --- | | Xavfsizlikni buzish natijasida olingan ma'lumotlardan noto'g'ri foydalanish tas’irni baholashni qasyi turiga mansub? | | Bilvosita |   **№ 89.** |
| |  | | --- | | Identifikatsiya jarayonini amalga oshirishning eng muvaffaqiyatli algoritmida birinchi qadam qanday? | | Potensial risklarni aniqlash |   **№ 90.** |
| |  | | --- | | Identifikatsiya jarayonini amalga oshirishning eng muvaffaqiyatli algoritmi nechta qadamdan iborat? | | 6 |   **№ 91.** |
| |  | | --- | | Aktivlarni chuqur aniqlash va baholashni, ushbu aktivlarga nisbatan tahdidlarni va zaifliklarni baholashni o'z ichiga oladigan jarayon bu qaysi? | | Axborot xavfsizligi riskini batafsil baholash |   **№ 92.** |
| |  | | --- | | Axborot xavfsizligi riskini batafsil baholashning yakuniy bosqichi – bu qaysi? | | Riskning umumiy bahosi |   **№ 93.** |
| |  | | --- | | Aktivlarni qayta shakllantirishdagi qulaylik, personal tomonidan yuzaga keluvchi tahdidlar ko'rib chiqilganda zaiflik hisobiga maqsadga erishish omili nimaga ta’sir qiladi? | | Muayyan tahdid ehtimolligiga |   **№ 94.** |
| |  | | --- | | Amaliy risk boshqaruvi nechta jarayonni o’z ichiga oladi? | | 4 |   **№ 95.** |
| |  | | --- | | Bu yondashuv ko'pchilik xalqaro va rus standartlari va qoidalari nuqtai nazaridan afzaldir. Gap qaysi yondashuv haqida ketmoqda? | | Belgilangan metodika bo'yicha rasmiy baholash |   **№ 96.** |
| |  | | --- | | Bu yondashuv xavflarni baholash sohasida malakaga ega bo'lgan ekspertlar guruhining risklarni baholashni, shuningdek, baholash o'tkazilayotgan axborot xavfsizligi ob'ekti / jarayoni / tizimining ishlash zaruriy xususiyatlarini tushunishini nazarda tutadi. Gap qaysi yondashuv haqida ketmoqda? | | Ekspertlar guruhining bahosi |   **№ 97.** |
| |  | | --- | | Bu yondashuv kompaniyaning mutaxassislari tomonidan riskni baholashdan bosh tortishni va tartibga soluvchilar, jamoalar, soha ishtirokchilari tomonidan ishlab chiqilgan mavjud tahdid modellari, xavf registrlari va xavfsizlik standartlaridan foydalanishni nazarda tutadi.  Gap qaysi yondashuv haqida ketmoqda? | | Qabul qilingan standartlar/modellardan foydalanish |   **№ 98.** |
| |  | | --- | | Baholashning bu turi dastlab ko'plab mutaxassislarga juda yaqin, chunki deyarli har bir kishi ma'lum qarorlar qabul qilishda kundalik hayotida bu baholash usulini qo'llaydi. Gap qaysi yondashuv haqida ketmoqda? | | Norasmiy / intuitiv baholash |   **№ 99.** |
| |  | | --- | | Aktivni ishlab chiqish, saqlash yoki almashtirish nuqtai nazaridan har bir axborot aktiviga investitsiya darajasi qaysi jarayon omili hisoblanadi? | | Riskni yuqori darajali baholash |   **№ 100.** |
| |  | | --- | | Riskni yuqori darajali baholashni boshlashdan maqsad nima? | | Biznes uzluksizligi bilan bog’liq rejalar bilan sinxronlashtirish |   **№ 101.** |
| |  | | --- | | Sug'urta risklarni boshqarish usullarining qaysi guruhiga kiradi? | | xavflardan qochish usullari |   **№ 102.** |
| |  | | --- | | CRAMM usuli doirasida avtomatlashtirilgan protseduralarni bajarish quyidagilardan qaysini o'z ichiga oladi? | | Ketma-ket uchta bosqichni ajratish. |   **№ 103.** |
| |  | | --- | | CRAMM usuli doirasida birinchi bosqichda nima amalga oshiriladi? | | Himoya tizimining bazaviy darajasining qo'llaniladigan vositalarini tahlil qilish va risklar darajasiga muvofiqligi to'g'risida xulosa chiqariladi |   **№ 104.** |
| |  | | --- | | CRAMM usuli doirasida, agar resurslarning kritik darajasi juda past bo'lsa, tizimga qanday xavfsizlik talablari qo‘yiladi? | | Tizimga minimal xavfsizlik talablari quyiladi |   **№ 105.** |
| |  | | --- | | CRAMM usuli doirasida ikkinchi bosqichda nimalar bajariladi? | | Xavfsizlik tahdidlari va zaifliklari tahlili amalga oshirish |   **№ 106.** |
| |  | | --- | | CRAMM usuli doirasida uchinchi bosqichda nimalar bajariladi? | | Risklarni boshqarish muammosi hal qilinadi, tegishli qarshi choralar tanlash |   **№ 107.** |
| |  | | --- | | CRAMM ning qarshi choralar uchun bir nechta variantlarni avtomatik ravishda yaratish imkoniyatini belgilang. | | 1000 dan ortiq |   **№ 108.** |
| |  | | --- | | CRAMM usulining kuchli tomonlarini belgilang. | | Bu yaxshi tuzilgan va keng miqyosda sinovdan o'tgan risklarni tahlil qilish usuli bo'lib, haqiqiy amaliy natijalarni olish imkonini beradi |   **№ 109.** |
| |  | | --- | | CRAMM usulining kamchiliklari keltirilgan javobni belgilang. | | Maxsus tayyorgarlik va yuqori malakani talab qiladi |   **№ 110.** |
| |  | | --- | | Potentsial zararni baholash uchun CRAMM qanday parametrlardan foydalanishni tavsiya qiladi? | | Tashkilotning obro'siga putur yetkazish, jismoniy shaxslarning shaxsiy ma'lumotlarini oshkor qilish bilan bog'liq zarar, resurslarni tiklash bilan bog'liq moliyaviy yo'qotishlar |   **№ 111.** |
| |  | | --- | | RiskWatch usulida risklarni baholash va boshqarish mezonlari sifatida qanday ko‘rsatgichlardan foydalaniladi? | | Kutiladigan yillik yo'qotishlar (Annual Loss Expectancy, ALE) va investitsiyalarning qaytish bahosi (Return on Investment, ROI) |   **№ 112.** |
| |  | | --- | | RiskWatch metodologiyasida quyidagi xavflarni baholash va boshqarish mezonlaridan qaysi biri qo'llaniladi? | | Yillik yo'qotishlar (Annual Loss Expectancy, ALE) va investitsiya qaytishini baholash (Return on Investment, ROI) |   **№ 113.** |
| |  | | --- | | RiskWatch usuli doirasida avtomatlashtirilgan protseduralarni bajarish quyidagilardan qaysi birini o'z ichiga oladi? | | To'rtta ketma-ket bosqichlarni ajratish. |   **№ 114.** |
| |  | | --- | | RiskWatch usuli doirasida birinchi bosqichda nima amalga oshiriladi? | | Tadqiqot predmetining ta'rifi. Tashkilot turi, o'rganilayotgan tizimning tarkibi (umumiy ma'noda), bazaviy xavfsizlik talablari |   **№ 115.** |
| |  | | --- | | RiskWatch usuli doirasidagi ikkinchi bosqich mohiyatini belgilang. | | Tizimning o'ziga xos xususiyatlarini tavsiflovchi ma'lumotlarni kiritish. resurslar, yo'qotishlar va hodisalar sinflari, aniqlangan har bir tahdidning paydo bo'lish chastotasi, zaiflik darajasi va resurslarning qiymatini aniqlash |   **№ 116.** |
| |  | | --- | | RiskWatch usuli doirasida uchinchi bosqichda nima amalga oshiriladi? | | Xavfni miqdoriy baholash |   **№ 117.** |
| |  | | --- | | RiskWatch usuli doirasida to‘rtinchi bosqichda qanday ish amalga oshiriladi? | | Hisobotlarni yaratish |   **№ 118.** |
| |  | | --- | | Quyidagi keng tarqalgan risklarni tahlil qilish usullaridan qaysi biri xavfni sifat jihatidan baholash usulidan foydalanadi (masalan, “yuqori”, “o‘rta”, “past” shkalasi bo‘yicha)? | | CRAMM |   **№ 119.** |
| |  | | --- | | Xavf omillarini kuzatish va qayta ko'rib chiqish uchun qanday kirish ma'lumotlaridan foydalaniladi? | | Risklarni boshqarish harakatlari natijasida olingan risklar haqidagi barcha ma'lumotlar |   **№ 120.** |
| |  | | --- | | Xavf omillarini monitoring va qayta ko'rib chiqishdan keyin qanday chiqish ma'lumotlari shakllantiriladi? | | Tashkilot kontekstidagi har qanday o'zgarishlarni dastlabki bosqichda aniqlash va xavfning umumiy tuzilishini ko'rib chiqishni qo'llab-quvvatlash uchun xavflar va ularning omillari monitoringi qayta ko'rib chiqilishi |   **№ 121.** |
| |  | | --- | | Risk boshqaruvida doimiy monitoring nima uchun zarur? | | Tahdidlar, zaifliklar, ehtimolliklar yoki oqibatlar hech qanday ko'rsatmasiz kutilmaganda o'zgarishi mumkin. Risklar statik bo'lib qolmaydi |   **№ 122.** |
| |  | | --- | | Tashkilotlar qanday omillarning doimiy monitoringini ta'minlashi lozim deyiladi? | | Xatarlarni boshqarish doirasiga kiritilgan yangi aktivlarni |   **№ 123.** |
| |  | | --- | | Tashkilotlar qanday omillarning doimiy monitoringini ta'minlashi lozim? | | Tashkilot tashqarisida va ichida faol bo'lishi mumkin bo'lgan hali baholanmagan yangi tahdidlar |   **№ 124.** |
| |  | | --- | | Tashkilotlar qanday omillarning doimiy monitoringini olib borishi talab etiladi? | | Yangi yoki kuchaygan zaifliklarning tahdidlarga ushbu yangi yoki o'zgartirilgan zaifliklardan foydalanishga imkon berishi ehtimolini |   **№ 125.** |
| |  | | --- | | Xavf omillarini monitoring qilish, tahlil qilishda e'tibor qaratilishi lozim bo’lgan jihatlar qaysi? | | Huquqiy kontekst, raqobat konteksti, riskni baholashga yondashuv, aktivlar qiymati va toifalari, ta'sir mezonlari, xavfni baholash mezonlari, xavfni qabul qilish mezonlari, operatsion aktivlarning umumiy qiymati, zarur resurslar |   **№ 126.** |
| |  | | --- | | Potensial xavfni kamaytirish strategiyalari nimani ichiga oladi? | | Riskni kamaytirish |   **№ 127.** |
| |  | | --- | | Potensial xavfni kamaytirish strategiyalari nimani ichiga oladi? | | Riskni sug'urtalashni |   **№ 128.** |
| |  | | --- | | Risklarni boshqarish bosqichlaridan biri bu qaysi? | | Aktivlarni identifikatsiya qilish |   **№ 129.** |
| |  | | --- | | Quyidagilardan qaysi biri risklarni boshqarish bosqichlariga tegishli? | | Tahdid tahlili |   **№ 130.** |
| |  | | --- | | Tahdidlarni tahlil qilishning birinchi bosqichini belgilang? | | Tahdidlarni identifikasiyalash |   **№ 131.** |
| |  | | --- | | Xatarlarni baholash qanday savollarga javob berishga imkon beradi? | | Mavjud xavflar qabul qilinadimi |   **№ 132.** |
| |  | | --- | | 27000 oilasiga mansub xalqaro standartlar asosida qabul qilingan Axborot xavfsizligiga oid standartlar soni nechta? | | 5 |   **№ 133.** |
| |  | | --- | | O'z DSt ISO / IEC 27001: 2009 standarti nimani belgilaydi? | | Axborot xavfsizligini boshqarish tizimlari. Talablarni. |   **№ 134.** |
| |  | | --- | | O'z DSt ISO / IEC 27002: 2008 standarti nimani belgilaydi? | | Axborot xavfsizligini boshqarishning amaliy qoidalarini |   **№ 135.** |
| |  | | --- | | O'z DSt ISO / IEC 27003: 2014 standarti nimani belgilaydi? | | Axborot xavfsizligini boshqarish tizimini joriy qilish bo'yicha qo'llanmani |   **№ 136.** |
| |  | | --- | | O'z DSt ISO / IEC 27004: 2014 standarti nimani belgilaydi? | | Axborot xavfsizligini boshqarish tizimining samaradorligini o'lchashni |   **№ 137.** |
| |  | | --- | | O'z DSt ISO / IEC 27005: 2016 standarti nimani belgilaydi? | | Axborot xavfsizligi risklarini boshqarishni |   **№ 138.** |
| |  | | --- | | O'z DSt ISO / IEC 27005: 2016 bo'yicha xavf tahlili deganda nima tushuniladi? | | Tavakkalchilikning mohiyatini tushunish va xavf darajasini aniqlash jarayoni. |   **№ 139.** |
| |  | | --- | | O'z DSt ISO / IEC 27005: 2016 bo'yicha xavf mezoni nima? | | Xatarning ahamiyatliligi bilan baholanadigan qoidalar |   **№ 140.** |
| |  | | --- | | O'z DSt ISO / IEC 27005: 2016 bo'yicha riskni qayta ishlash nima? | | Xavfni o'zgartirish jarayoni |   **№ 141.** |
| |  | | --- | | O'z DSt ISO / IEC 27005: 2016 bo'yicha xavfni baholash nima? | | Xatar va/yoki kattaligi maqbul yoki ruxsat etilgan darajada ekanligini aniqlash uchun xavf tahlili natijalarini xavf mezonlari bilan solishtirish jarayoni |   **№ 142.** |
| |  | | --- | | Axborot xavfsizligi xavfi deganda nima tushuniladi? | | Tahdidlarni amalga oshirishda axborot aktivlari yoki axborot aktivlari guruhining zaifligidan foydalangan holda tashkilotga yetkazilgan zarar |   **№ 143.** |
| |  | | --- | | Axborot xavfsizligi risklarini boshqarish jarayoni nimaga yordam beradi? | | Xatarlarni biznes oqibatlari va ularning yuzaga kelish ehtimoli nuqtai nazaridan baholash, yuzaga kelishi mumkin bo'lgan xavflarni kamaytirish bo'yicha harakatlar uchun ustuvor yo'nalishlarni belgilash |   **№ 144.** |
| |  | | --- | | Axborot xavfsizligi risklarini boshqarish jarayoni qanday bosqichlardan iborat? | | Kontekstni aniqlash, xavfni aniqlash, xavfni tahlil qilish, xavfni baholash, xavfni qayta ishlash |   **№ 145.** |
| |  | | --- | | Axborot xavfsizligini boshqarish tizimi qanday bosqichlardan iborat? | | Rejalashtirish, amalga oshirish, tekshirish, harakat qilish |   **№ 146.** |
| |  | | --- | | Xatarlarni qabul qilish mezonlari nima asosidabelgilanadi? | | Biznes mezonlari, qonunchilik va tartibga solish jihatlari, operatsiyalar, texnologiya, moliya, ijtimoiy va gumanitar omillar |   **№ 147.** |
| |  | | --- | | Tashkilotning axborot xavfsizligini boshqarish darajalarini belgilang? | | Strategik boshqaruv, taktik boshqaruv, operativ boshqaruv |   **№ 148.** |
| |  | | --- | | Strategik boshqaruv darajasining funksional komponentlari qaysilar? | | Tashkilotning texnik siyosatini, axborot xavfsizligi xizmatini, huquqiy nazoratni ta'minlash |   **№ 149.** |
| |  | | --- | | Taktik rejalashtirish darajasining funksional komponentlarini belgilang. | | Axborot xavfsizligi siyosatini shakllantirish, nazorat qilish, tahlil qilish, ekspertiza, tekshirish. |   **№ 150.** |
| |  | | --- | | Operativ rejalashtirish darajasining funksional komponentlarini belgilang. | | Monitoring, maxsus himoya vositalarini nazorat qilish, nazorat qilish, boshqarish, avtomatlashtirilgan tizim vositalarini boshqarish. |   **№ 151.** |
| |  | | --- | | Tashkilotda axborot xavfsizligini boshqarish komponentlarini belgilang. | | AX boshqaruv jarayonining o'zi va tashkilotning AX boshqaruv tizimi (AXBT). |   **№ 152.** |
| |  | | --- | | Axborot xavfsizligini boshqarish tizimining uslubiy asosi to‘g‘ri ko’rsatilgan qatorni toping? | | Axborot xavfsizligini boshqarish doirasidagi jarayonli yondashuv |   **№ 153.** |
| |  | | --- | | Axborot xavfsizligini boshqarish tizimini yaratish va joriy etish strategiyasi bu nima? | | Yagona axborot xavfsizligini boshqarish tizimini qurish va joriy etish, axborot xavfsizligini boshqarish jarayonlarini alohida qurish va amalga oshirish, keyinchalik ularni axborot xavfsizligini yagona boshqaruv tizimiga integratsiya qilish |   **№ 154.** |
| |  | | --- | | Risklarni boshqarish (RB) tamoyillari to‘g‘ri keltirilgan qatorni belgilang. | | Integratsiyalashgan, tuzilgan va murakkab, moslashuvchan, keng qamrovli, dinamik, barcha mavjud ma'lumotlar, Inson va madaniy omillar, doimiy takomillashtirish |   **№ 155.** |
| |  | | --- | | Risklarni boshqarishda “integratsiyalashgan” tamoyilini to‘g‘ri ochib beruvchi qatorni ajratib ko‘rsating. | | Risklarni boshqarish har qanday tashkilot biznesining ajralmas qismidir |   **№ 156.** |
| **Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari** |
| |  | | --- | | Risklarni boshqarishda “Strukturaviy va murakkab” tamoyilini to'g'ri ochib beruvchi qatorni ajratib ko'rsating | | Xatarlarni boshqarishga o'ylangan va tushunarli yondashuv kamchiliklarni bartaraf qiladi va taqqoslanadigan natijalarni qamrab oladi |   **№ 157.** |
| |  | | --- | | Risklarni boshqarishda “Moslashuvchan” tamoyilini to'g'ri ochib beruvchi qatorni ajratib ko'rsating | | Xatarlarni boshqarish tuzilmasi va jarayoni tashkilotning maqsadlari bilan bog'liq tashqi va ichki kontekstiga muvofiq ishlab chiqilgan va moslashtirilgan. |   **№ 158.** |
| |  | | --- | | Risklarni “kompleks” boshqarish tamoyilini to‘g‘ri ochib beruvchi qatorni ajratib ko‘rsating. | | Manfaatdor tomonlarning tegishli va o'z vaqtida jalb etilishi ularning bilimlari, qarashlari va tasavvurlarini hisobga olish imkonini beradi. Bu xabardorlikni oshirish va xavflarni boshqarishda xabardor bo’lishiga olib keladi. |   **№ 159.** |
| |  | | --- | | Risklarni boshqarishda “Dinamik” tamoyilini to'g'ri ochib beruvchi qatorni ajratib ko'rsating | | Tashkilotning tashqi va ichki konteksti o'zgarganda xavflar paydo bo'lishi, o'zgarishi yoki yo'qolishi mumkin. Risklarni boshqarish ushbu o'zgarishlar va hodisalarni tegishli va o'z vaqtida ogohlantiradi, aniqlaydi, tasdiqlaydi va javob beradi. |   **№ 160.** |
| |  | | --- | | Xatarlarni boshqarishda “Barcha mavjud ma'lumotlar” tamoyilini to'g'ri ochib beradigan qatorni ajratib ko'rsating | | Xatarlarni boshqarish bo'yicha ma'lumotlar tarixi va joriy ma'lumotlarga hamda kelajakdagi taxminlarga asoslanadi. Risklarni boshqarish bunday ma'lumotlar va taxminlar bilan bog'liq har qanday o'zgarishlar va noaniqliklarni aniq ko'rib chiqadi. Ma'lumotlar o'z vaqtida, aniq va qaror qabul qiluvchilar uchun ochiq bo'lishi kerak |   **№ 161.** |
| |  | | --- | | Risklarni boshqarishda “Inson va madaniy omillar” tamoyilini to'g'ri ochib beruvchi qatorni ajratib ko'rsating | | Inson xulq-atvori va madaniyati har bir daraja va bosqichda risklarni boshqarishning barcha jihatlariga sezilarli drajada ta'sir qiladi |   **№ 162.** |
| |  | | --- | | Risklarni boshqarishda “Doimiy takomillashtirish” tamoyilini to'g'ri ochib beruvchi qatorni ajratib ko'rsating | | Risklarni boshqarish trening va tajriba orqali doimiy ravishda takomillashtiriladi |   **№ 163.** |
| |  | | --- | | Korxona yoki tashkilot aktivlarining qiymatini baholash maqsadini belgilang. | | aktiv ahamiyatini baholash va aktivlarni himoya qilishning zaruriy darajasini aniqlash |   **№ 164.** |
| |  | | --- | | Aktivlar nechta o'lchov asosida baholanadi? | | 3 |   **№ 165.** |
| |  | | --- | | Aktivlarni baholashning uch o'lchovi bu qaysilar? | | Maxfiylik, yaxlitlik va mavjudlik |   **№ 166.** |
| |  | | --- | | Aktivlarni baholash usullarini belgilang. | | sifat va miqdoriy baholash |   **№ 167.** |
| |  | | --- | | Sifat darajasi bo'yicha baholashning darajalarini aniqlang. | | Ahamiyatsiz, Past, O'rtacha, Yuqori, Halokatli |   **№ 168.** |
| |  | | --- | | Zaiflik tahlili mohiyatini aniqlang. | | Tashkilotning mumkin bo'lgan zaif tomonlarini sanab o'tish va ularni "kuchliligi" ga qarab toifalarga ajratish |   **№ 169.** |
| |  | | --- | | Zaifliklar toifalarini belgilang. | | Texnik, texnologik, tashkiliy |   **№ 170.** |
| |  | | --- | | Loyihalashda xatolik, ma'muriy xato qaysi zaiflik toifasiga kiradi? | | Texnologik |   **№ 171.** |
| |  | | --- | | Aktivni sifat bo'yicha baholashda dastlabki xavfsizlik darajasi qachon “yuqori” deyiladi? | | Agar aktivlarning kamida 70 foizi "yuqori" darajaga to'g'ri kelsa |   **№ 172.** |
| |  | | --- | | Aktivni sifat bo'yicha baholashda dastlabki xavfsizlik darajasi qachon “o’rtacha” deyiladi? | | Agar aktiv 1-band shartlarini bajarilmasa va uning xususiyatlarining kamida 70% i "o'rtacha" dan past bo'lmagan darajaga to'g'ri kelsa |   **№ 173.** |
| |  | | --- | | Aktivni sifat bo'yicha baholashda dastlabki xavfsizlik darajasi qachon “past” deyiladi? | | Agar aktivlar 1 va 2 -bandlar bo'yicha shartlar bajarilmasa, ya'ni 70% dan kam ko'rsatkichlar "o'rtacha" dan past darajaga to'g'ri kelsa |   **№ 174.** |
| |  | | --- | | Axborot xavfsizligining xavflarini baholash tartibi qanday aniqlanadi? | | Axborot xavfsizligiga qo‘yiladigan talablar xavflarni muntazam baholash yordamida aniqlanadi |   **№ 175.** |
| |  | | --- | | Axborot xavfsizligini joriy qilishning tayanch nuqtasi qaysi javobda to‘g‘ri ko‘rsatilgan? | | Axborot xavfsizligini boshqarish uchun amal qilinadigan prinsiplar sifatida qabul qilinishi va uni joriy qilish uchun tayanch nuqta bo‘lib xizmat qilishi mumkin. |   **№ 176.** |
| |  | | --- | | Rejalashtirish (AXBTni ishlab chiqish) nima? | | Tashkilotning umumiy siyosati va maqsadlarida e’lon qilingan natijalarga erishish maqsadida siyosat va maqsadlarni belgilash, xatarlarni boshqarish va axborot xavfsizligini takomillashtirish bilan bog‘liq bo‘lgan jarayonlar va protseduralarni aniqlash |   **№ 177.** |
| |  | | --- | | Amalga oshirish (AXBTni joriy etish va uning ishlashi) deganda nimani tushunasiz? | | AXBT siyosati, metodlari, jarayonlari va protseduralarini joriy etish va uning ishlashi |   **№ 178.** |
| |  | | --- | | Tekshirish (AXBT monitoringi va tahlili) deganda nimani tushunasiz? | | Jarayonlarning AXBT siyosati va maqsadlariga muvofiqligini baholash va zarurat bo‘lganida samaradorligini o‘lchash |   **№ 179.** |
| |  | | --- | | Harakat (AXBTni qo‘llab-quvvatlash va takomillashtirish) deganda nimani tushunasiz? | | AXBT ichki auditlari natijalariga, rahbariyat tomonidan qilingan tahlil yoki uzluksiz takomillashtirish maqsadida boshqa manbalardan olingan ma’lumotlarga asoslangan tuzatuvchi va ogohlantiruvchi harakatlarni bajarish |   **№ 180.** |
| |  | | --- | | AXBTni tuzishdan maqsad nima? | | Xavfsizlikni boshqarishning axborot aktivlarini muhofaza qilish uchun mo‘ljallangan va manfaatdor tomonlarning ishonchini kafolatlaydigan tegishli chora-tadbirlarini tanlash jarayonlari va protseduralarini joriy etish |   **№ 181.** |
| |  | | --- | | Tashkilotda xatarlarni baholashga yondashishni aniqlashda nima amalga oshiriladi? | | AXBT uchun mos keladigan xatarlarni baholash uslubiyatini aniqlash, shuningdek, axborot xavfsizligi sohasida tashkilot faoliyatini ta’minlash |   **№ 182.** |
| |  | | --- | | Tashkilot AXBT hujjatlarining hajmi nimalarga bog‘liq? | | Tashkilotning miqyosi va uning faoliyat turi, boshqaruv amalga oshiriladigan tizim xavfsizligi talablarining qo‘llanish sohasi va murakkabliligi |   **№ 183.** |
| |  | | --- | | Biznesning boshqa muhim aktivlari kabi qiymatga ega bo‘lgan aktiv nima? | | Axborot |   **№ 184.** |
| |  | | --- | | Axborot xavfsizligiga qanday yo‘l bilan erishiladi? | | Dasturiy ta’minotning siyosatlari, metodlari, protseduralari, tashkiliy tuzilmalari va dasturiy ta’minot funksiyalari tomonidan taqdim etilishi mumkin bo‘lgan axborot xavfsizligini boshqarish bo‘yicha tadbirlarning tegishli kompleksini amalga oshirish |   **№ 185.** |
| |  | | --- | | AXB ning bazaviy jarayonlari nima? | | Axborot xavfsizligi risklarini boshqarish, axborot xavfsizligi insidentlarini boshqarish |   **№ 186.** |
| |  | | --- | | Biznes uzluksizligini boshqarish kompleks boshqaruv jarayoni sifatida nimani o'z ichiga oladi? | | Tashkilotning ishida buzilishlar aniqlangan taqdirda tiklanish yoki uning faoliyatini davom ettirishni boshqarish |   **№ 187.** |
| |  | | --- | | Biznes uzluksizligini boshqarish jarayonini nechta yo‘nalishga bo'lish mumkin? | | Biznes jarayonlarining insidentlarga chidamliligini ta'minlash, tashkilotning biznesini tiklash |   **№ 188.** |
| |  | | --- | | Biznes jarayonlarining insidentlarga chidamliligini ta’minlashdan maqsad nima? | | Xavfli hodisaning yuzaga kelish ehtimolini kamaytirishda va inqirozga qarshi profilaktika choralarini ishlab chiqish va amalga oshirish |   **№ 189.** |
| |  | | --- | | Biznes faoliyatni tiklanishini ta’minlash nimadan iborat? | | Oldindan sodir bo'lgan hodisaning salbiy ta'sirini kamaytirish va tuzatish |   **№ 190.** |
| |  | | --- | | Biznes uzluksizligini boshqarish jarayonining birinchi asosiy jihati keltirilgan qatorni ajratib ko'rsating. | | Vaqt o'tishi bilan oqibatlarning ehtimoli va yuzaga kelishi nuqtai nazaridan tashkilot duch keladigan xatarlarni tushunish, shu jumladan muhim biznes jarayonlarini aniqlash va ustuvorliklarni belgilash |   **№ 191.** |
| |  | | --- | | Biznes uzluksizligini boshqarish jarayonining ikkinchi asosiy jihati keltirilgan qatorni ajratib ko'rsating. | | Muhim biznes jarayonlarida ishtirok etadigan barcha aktivlarni aniqlash |   **№ 192.** |
| |  | | --- | | Biznes uzluksizligini boshqarish jarayonining uchinchi asosiy jihati keltirilgan qatorni ajratib ko'rsating. | | Hodisaga asoslangan uzilishlarning ta'sirini tushunish va tashkilotning biznes maqsadlariga mos keladigan ma'lumotlarni qayta ishlash vositalari va usullarini tanlash. |   **№ 193.** |
| |  | | --- | | Tahdid aniqlanganidan keyingi baholanuvchi jarayon bu qaysi? | | Uni amalga oshirish ehtimolini |   **№ 194.** |
| |  | | --- | | Himoya choralari narxini tahlil qilishda e'tiborga olinuvchi jihatlarni belgilang. | | Uskunalar sotib olish xarajatlarini |   **№ 195.** |
| |  | | --- | | Risk tahdiddan nimasi bilan farqlanadi? | | Mumkin bo'lgan yo'qotishlarni miqdoriy baholash va (ehtimol) tahdidning amalga oshishi ehtimolini baholashning mavjudligi bilan |   **№ 196.** |
| |  | | --- | | Xavf ma'lum bir manbaga tahdidni amalga oshirish mumkin bo'lgan zaiflik sifatida aniqlanganmi? | | Ha |   **№ 197.** |
| |  | | --- | | Axborot xavfsizligi siyosatini ishlab chiqishda qanday asosiy qoidaga amal qilish zarur? | | Muayyan aktivni himoya qilish qiymati aktivning o'z qiymatidan oshmasligi kerak |   **№ 198.** |
| |  | | --- | | CRAMM aniqlangan xavflar va ularning darajalariga mos keladigan qarshi choralari qatorida nechta umumiy tavsiyalar mavjud? | | 300 ga yaqin |   **№ 199.** |
| |  | | --- | | Axborot xavfsizligi sohasida risk deb nimaga aytiladi? | | axborot tizimining xavfsizligini buzish natijasida yo'qotishlarning ehtimoliy miqdori |   **№ 200.** |
| |  | | --- | | CRAMM zaiflik reytingi shkalasining qaysi qiymati o'rtacha har uch yilda bir marta sodir bo'ladigan insidentga mos keladi? | | Past | |
|  |