**FAN BO‘YICHA TALABALAR BILIMINI BAHOLASH VA NAZORAT QILISHGA DOIR TEST SAVOLLARI**

**№ 1.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Risk ta‘rifi to‘g‘ri keltirilgan qatorni belgilang. |
| noaniqlikning maqsadlarga ta'siri |
| hakerlik harakati |
| yuzaga keluvchi tahlika |
| yuz bergan insident |

**№ 2.**

**Manba:**  **1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| …. bu xavfsizlik tizimining kamchiligi bo‘lib, xavfni ro'yobga chiqarishga imkon beradi. Bu tushuncha quyidagilardan qay biriga tegishli? |
| Zaiflik |
| Parollar |
| Himoyasiz tizim |
| Hodisa |

**№ 3.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Axborot xavfsizligi xavflarini (risk) boshqarishga kirish fani maqsadiga zid bo’lgan qatorni belgilang. |
| Faqat risklarni aniqlash va hisoblash |
| Risklarni qayta ishlash, bartaraf etish usullarini tadbiq etish |
| Risklarni tahlil qilishga doir bilimlar va ko’nikmalar hosil qilish |
| Axborot xavfsizligi xavflarini aniqlash va vositalarini qo’llash |

**№ 4.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Risklarni boshqarishda xavfsizlik siyosatining eng asosiy vazifalaridan biri bu nima? |
| Himoya tizimida potensial xavfli nuqtalarni qidirib topish va ularni bartaraf etish |
| Risklarni tahlil qilishga doir bilimlar va ko’nikmalar hosil qilish |
| Risklarni hisoblash |
| Risklarni aniqlash va hisoblash |

**№ 5.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Axborot xavf xatarlari nuqtai nazaridan “noaniqlik” nimani anglatadi? |
| Ma'lumotlarning yetishmasligi (hatto qisman) |
| Mumkin bo'lgan hodisalar |
| Hodisaning oqibatlari |
| Dinamik ma’lumotlar |

**№ 6.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Axborot xavf xatarlari nuqtai nazaridan “Hodisa”ga bog‘liq bo‘lmagan tushunchani belgilang. |
| Ijtimoiy himoyalanish |
| Hodisa bir yoki bir necha marta sodir bo'lishi mumkin |
| Hodisa bir necha sabablarga ko'ra sodir bo'lishi mumkin |
| Hodisa, biror kutilmagan narsa sodir bo'lishidir |

**№ 7.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Standart operatsiyalar qatoriga qo‘shilmaydigan hamda xizmat holatini uzib qo‘yish yoki xizmat sifati yomonlashishi holatlariga olib keladigan har qanday hodisa bu nima? |
| Insident |
| Zaiflik |
| Hakerlik harakati |
| Yuzaga keluvchi tahlika |

**№ 8.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Zaiflik tushunchasi to’g’ri ko’rsatilgan qatorni belgilang? |
| Xavfsizlik tizimining kamchiligi, bu xavfni ro'yobga chiqarishga imkon beradi |
| Xavfni o'zgartirish chorasi |
| Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan kutilmagan hodisa |
| Tashkilot uchun eng qimmatli narsa |

**№ 9.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Aktiv tushunchasi to’g’ri ko’rsatilgan qatorni belgilang. |
| Tashkilot uchun eng qimmatli narsalar |
| Xavfni o'zgartirish chorasi |
| Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan kutilmagan hodisa |
| Xavfsizlik tizimining kamchiligi, bu xavfni ro'yobga chiqarishga imkon beradi |

**№ 10.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Boshqarish tushunchasi to’g’ri ko’rsatilgan qatorni belgilang. |
| Xavfni o'zgartirish chorasi |
| Tashkilot uchun eng qimmatli narsa |
| Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan kutilmagan hodisa |
| Xavfsizlik tizimining kamchiligi, bu xavfni ro'yobga chiqarishga imkon beradi |

**№ 11.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Risklarni boshqarish vositalarini belgilang. |
| Riskni o'zgartirishga qaratilgan har qanday jarayonlar, siyosatlar, qurilmalar, protseduralar |
| Tahlil, teskari aloqa |
| Olingan ma'lumotlarni o'rganish, faraz va tavsiyalarni shakllantirish |
| Berilgan ma'lumotlarga bo'lgan munosabatini qabul qilish va qayd etish |

**№ 12.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Rikslar menejmenti nima? |
| Risk sohasidagi tashkilotni boshqarish va boshqarishning muvofiqlashtirilgan faoliyati |
| Olingan ma'lumotlarni o'rganish, faraz va tavsiyalarni shakllantirish |
| Berilgan ma'lumotlarga bo'lgan munosabatini qabul qilish va qayd etish |
| Jarayonni rejalashtirish |

**№ 13.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Axborot xavfsizligi xavfini boshqarish jarayoni tashkil etuvchilari to’liq ko’rsatilgan qatorni belgilang. |
| kontekstni aniqlash, riskni baholash, davolash, qabul qilish, ma'lumot almashish, monitoring |
| kontekstni aniqlash, riskni baholash, davolash |
| Teskari aloqa, Tahlil, Rejalashtirish |
| Rejalashtirish, kontekstni aniqlash, riskni baholash |

**№ 14.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Xavfni qayta ishlash samaradorligi nimaga bog’liq? |
| xavfni baholash natijalariga |
| xavf darajasiga |
| xavf manbasiga |
| jarayonni rejalashtirishga |

**№ 15.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Xavfli hodisaning yo'lini sababdan oqibatgacha tavsiflash va tahlil qilishning sxematik usulini belgilang. |
| “galstuk-babochka” tahlil usuli |
| “nosozlik daraxti” tahlil usuli |
| “Vaziyatlar daraxti” tahlil usuli |
| “Gammalash” tahlil usuli |

**№ 16.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Hodisa sabablarini nosozlik daraxti yordamida o'rganishni va voqealar daraxti yordamida oqibatlarini tahlil qilishni birlashtiruvchi tahlil usulini belgilang. |
| “galstuk-babochka” tahlil usuli |
| “nosozlik daraxti” tahlil usuli |
| “Vaziyatlar daraxti” tahlil usuli |
| “Gammalash” tahlil usuli |

**№ 17.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Asosiy yo'nalishi sabablar va xavfli hodisalar oqibatlari o'rtasidagi to'siqlarga qaratilgan tahlil usulini belgilang. |
| “galstuk-babochka” tahlil usuli |
| “nosozlik daraxti” tahlil usuli |
| “Vaziyatlar daraxti” tahlil usuli |
| “Gammalash” tahlil usuli |

**№ 18.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| “nosozlik daraxti” tahlil usuli |
| “Vaziyatlar daraxti” tahlil usuli |
| “Gammalash” tahlil usuli |

**№ 19.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| “Galstuk-babochka” tahlil usuli |
| “Vaziyatlar daraxti” tahlil usuli |
| “Gammalash” tahlil usuli |

**№ 20. 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Manba:**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. |
| “VA” mantiqiy elementi |
| “YOKI” mantiqiy elementi |
| “EMAS” mantiqiy elementi |
| Hodisa tahlil qilinmaydi |

**№ 21.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. |
| “YOKI” mantiqiy elementi |
| “VA” mantiqiy elementi |
| “EMAS” mantiqiy elementi |
| Hodisa tahlil qilinmaydi |

**№ 22.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. |
| Asosiy hodisa-tahlilni davom ettirishdan mantiq yo‘q |
| Hodisa tahlil qilinmaydi |
| Tahlil qilinishi kerak bo’lgan hodida |
| O‘tkazish-hodisa tahlilini boshqa sahifa yoki joyda davom ettirish |

**№ 23.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. |
| Hodisa tahlil qilinmaydi |
| Asosiy hodisa-tahlilni davom ettirishdan mantiq yo‘q |
| Tahlil qilinishi kerak bo’lgan hodida |
| O‘tkazish-hodisa tahlilini boshqa sahifa yoki joyda davom ettirish |

**№ 24.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. |
| Tahlil qilinishi kerak bo’lgan hodida |
| Hodisa tahlil qilinmaydi |
| Asosiy hodisa-tahlilni davom ettirishdan mantiq yo‘q |
| O‘tkazish-hodisa tahlilini boshqa sahifa yoki joyda davom ettirish |

**№ 25.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Nosozliklar daraxti tahlili diagrammasida ifodalanuvchi  element mohiyatini belgilang. |
| O‘tkazish-hodisa tahlilini boshqa sahifa yoki joyda davom ettirish |
| Hodisa tahlil qilinmaydi |
| Tahlil qilinishi kerak bo’lgan hodida |
| Asosiy hodisa-tahlilni davom ettirishdan mantiq yo‘q |

**№ 26.**

**Manba: 4-Ma‘ruza. Risklarni boshqarishda kontekst tushunchasi**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| chegarani aniqlash |
| xatolarni aniqlash |
| mezonni takomillashtirish |

**№ 27.**

**Manba: 4-Ma‘ruza. Risklarni boshqarishda kontekst tushunchasi**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Kontekst turlarini belgilang. |
| Ichki kontekst, Tashqi kontekst |
| Asosiy, ikkinchi darajali |
| xavfli, xavfsiz |
| ehtimoliy, aniq |

**№ 28.**

**Manba: 4-Ma‘ruza. Risklarni boshqarishda kontekst tushunchasi**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Tashqi kontekst to’g’ri keltirilgan qatorni belgilang. |
| Tashkilot o'z maqsadlariga erishmoqchi bo'lgan tashqi muhit |
| Tashkilot o'z maqsadlariga erishishga undaydigan ichki muhit |
| Siyosatlar, maqsadlar va ularga erishish strategiyalari |
| Tashkilot tomonidan qabul qilingan standartlar, ko'rsatmalar va modellar |

**№ 29.**

**Manba: 4-Ma‘ruza. Risklarni boshqarishda kontekst tushunchasi**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Ichki kontekst to’g’ri keltirilgan qatorni belgilang. |
| Tashkilot o'z maqsadlariga erishishga undaydigan ichki muhit |
| Tashkilot o'z maqsadlariga erishmoqchi bo'lgan tashqi muhit |
| Siyosatlar, maqsadlar va ularga erishish strategiyalari |
| Tashkilot tomonidan qabul qilingan standartlar, ko'rsatmalar va modellar |

**№ 30.**

**Manba: 4-Ma‘ruza. Risklarni boshqarishda kontekst tushunchasi**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| Asosiy, ikkinchi darajali |
| xavfli, xavfsiz |
| Ichki kontekst |

**№ 31.**

**Manba: 4-Ma‘ruza. Risklarni boshqarishda kontekst tushunchasi**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Asosiy, ikkinchi darajali |
| xavfli, xavfsiz |
| Tashqi kontekst |

**№ 32.**

**Manba: 4-Ma‘ruza. Risklarni boshqarishda kontekst tushunchasi**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Risklarni boshqarish maqsadiga zid bo’lgan qatorni belgilang. |
| identifikatsiya, autentifikatsiya |
| Insidentlarga javob rejasini tayyorlash |
| Biznesning uzluksizligi rejasini tayyorlash |
| Axborot xavfsizligini boshqarish tizimini qo'llab-quvvatlash |

**№ 33.**

**Manba: Manba: 4-Ma‘ruza. Risklarni boshqarishda kontekst tushunchasi**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Axborot xavfsizligi hodisasi natijasida tashkilotga yetkazilgan zarar yoki zarar darajasini belgilashda ishtirok etmaydigan tushunchani belgilang. |
| Tashkiliy choralar |
| Qonuniy, me'yoriy yoki shartnoma talablarini buzish |
| Jarayonning yomonlashuvi, nufuzga oid zarar |
| Ta'sir etilgan axborot aktivlarining tasniflash darajasi |

**№ 34.**

**Manba: Manba: 4-Ma‘ruza. Risklarni boshqarishda kontekst tushunchasi**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| Biznes mezonlari, huquqiy va tartibga soluvchi jihatlar, Operatsiyalar |
| Operatsiyalar, Texnologiya, Moliya, Ijtimoiy va gumanitar omillar |
| Biznes mezonlari, huquqiy va tartibga soluvchi jihatlar |

**№ 35.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Aktiv namunalari to’g’ri keltirilgan qatorni belgilang. |
| Xodimning ish stoli, noutbuk yoki telefoni, serverlar, qurilmalardagi ilovalar, qo'llab-quvvatlash tizimlari |
| axborot xavfsizligi hodisalarini kuzatish va ularga javob berish |
| identifikatorlar, parollar, qurilmalar, kitoblar |
| axborot xavfsizligi dasturi, loyihalar |

**№ 36.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| ISO 27001ni joriy qilishda tashkilotlarning bajarishi kerak bo'lgan birinchi qadam bu -… |
| axborot aktivlarini aniqlash |
| axborot xavfsizligi dasturi |
| loyihalarni rejalashtirish |
| axborot xavfsizligi hodisalarini kuzatish |

**№ 37.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| Administrator |
| Yurist |
| Xodim |

**№ 38.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Axborot aktivlarining turlarini belgilang. |
| Asosiy, yordamchi |
| Bazaviy, individual |
| Turdosh, xilmaxil |
| Doimiy, vaqtincha |

**№ 39.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Asosiy axborot aktivlari keltirilgan qatorni belgilang. |
| Biznes jarayonlari va faoliyati, axborot |
| Apparat taminot |
| Dasturiy ta'minot |
| Tashkiliy tuzilma |

**№ 40.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Yordamchi axborot aktivlari keltirilgan qatorni belgilang. |
| Apparat taminot, dasturiy ta'minot, tarmoq, xodimlar, sayt, tashkiliy tuzilma |
| tarmoq, xodimlar, sayt, tashkiliy tuzilma, axborot |
| Apparat taminot, dasturiy ta'minot, biznes jarayonlari |
| Operatsiyalar, Texnologiya, Moliya |

**№ 41.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Asosiy aktiv “axborot” tarkibiga kirmaydigan qatorni belgilang. |
| Qalbakilashtirilgan ma'lumotlar |
| Shaxsini xarakterlovchi ma'lumotlar |
| Tashkilot strategik ma'lumotlari |
| Tashkilot uchun qimmatli bo'lgan har qanday ma'lumot |

**№ 42.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Yordamchi aktiv “Apparat ta'minot” tarkibiga kirmaydigan qatorni belgilang. |
| To'plash, saqlash, qayta ishlash va uzatish uzoq davom etadigan qimmatli ma'lumotlar |
| Mobil uskunalar |
| Statsionar uskunalar |
| Ma'lumotni qayta ishlash uskunalari |

**№ 43.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Yordamchi aktiv “Dasturiy ta'minot” tarkibiga kirmaydigan qatorni belgilang. |
| Ma'lumotni qayta ishlash uskunalari |
| Xizmat ko'rsatish yoki boshqaruv dasturi |
| Standart dasturiy ta'minot |
| Operatsion tizim |

**№ 44.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Yordamchi aktiv “Shaxs” to’g’ri va to’liq keltirilgan qatorni belgilang. |
| Qaror qabul qiluvchi, Foydalanuvchilar, Operatsion va texnik xodimlar, Ishlab chiquvchi |
| Qaror qabul qiluvchi, Foydalanuvchilar, qurilmalar |
| Operatsion va texnik xodimlar, jarayonlar |
| xavfsizlik bo’limi boshlig’i |

**№ 45.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Aktivlarni aniqlashning eng yaxshi usuli bu nima? |
| mulk egalari bilan suhbat |
| Apparat ta’minotdan foydalanish |
| dasturiy ta’minotdan foydalanish |
| yangiliklarni kuzatish |

**№ 46.**

**Manba: 2-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) baholash metodlari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| “Modullash” tahlil usuli |
| “galstuk-babochka” tahlil usuli |
| “Gammalash” tahlil usuli |

**№ 47.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo’yicha asosiy tushunchalar, fanning maqsadi va vazifalari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Muayyan holatlarning paydo bo'lishi yoki o'zgarishi nima deb ataladi? |
| Hodisa |
| Jarayon |
| Yangilanish |
| Rivojlanish |

**№ 48.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo’yicha asosiy tushunchalar, fanning maqsadi va vazifalari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Hodisa (yoki insident)ning qanday turlari mavjud? |
| Normal, Avariyaviy |
| Bazaviy, individual |
| Turdosh, xilmaxil |
| Doimiy, vaqtincha |

**№ 49.**

**Manba: 4-Ma‘ruza. Risklarni boshqarishda kontekst tushunchasi**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Quyidagi ta’rifga mos kalit so’zni belgilang. |
| Kontekst dastlab \_\_\_\_\_\_\_\_\_\_\_\_ riskni baholashda o'rnatiladi. |
| Yuqori darajali |
| Past darajali |
| O’rta darajali |
| Ahamiyatsiz |

**№ 50.**

**Manba: 7-Ma‘ruza. AX risklarini qayta ishlash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| riskni uzatish |
| riskni qabul qilish |
| muvofiqlashtirish |

**№ 51.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| Tashqi tahdidlar |
| Ichki tahdidlar |
| Dasturiy ta’minot zaifliklari |

**№ 52.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Korxonani nomi, nufuzi va imidji kabilar qimmatli aktivlarni qaysi turiga mansub hisoblanadi? |
| Korxonani nomoddiy manbalari |
| Korxonaning moddiy manbalari |
| Axborot resurslari |
| Xizmatlar |

**№ 53.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Korxonadagi kompyuter qurilmalari, telekommunikatsiya va boshqa qurilmalari qimmatli aktivlarni qaysi turiga mansub hisoblanadi? |
| Korxonaning moddiy manbalari |
| Korxonani nomoddiy manbalari |
| Axborot resurslari |
| Xizmatlar |

**№ 54.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| Tashkilot xodimi hisoboti |
| Administrator bayonnomasi |
| Rahbar bayonnomasi |

**№ 55.**

**Manba: 5- Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| … - 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 |
| Aktivlarni identifikatsiyalash |
| Risklarni baholash |
| Risklarni tahlil |

**№ 56.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Aktivlar qaysi o’lchovlar asosida baholanadi? |
| Maxfiylik, yaxlitlik va mavjudlik. |
| Kafolat, to’lalik va foydalanuvchanlik |
| Yetkazuvchanlik, kafolat va butunlilik |
| Qiymatlilik, kafolat va mavjudlik |

**№ 57.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Sifat darajasiga ko’ra baholashda nechta darajadan foydalanish eng qulay hisoblanadi? |
| 5 |
| 4 |
| 6 |
| 3 |

**№ 58.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Tashkilotning mumkin bo'lgan zaif tomonlarini sanab o'tish va ularni "kuchliligi" ga qarab toifalarga ajratish qanday jarayon hisoblanadi? |
| Zaiflilik tahlili |
| Aktivlar identifikatsiyasi |
| Tahdidlarni baholash |
| Aktivlarni baholash |

**№ 59.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Zaifliklar qanday toifalarga ajraladi? |
| Texnik, texnologik va tashkiliy |
| Dasturiy, dasturiy-texnik va qurilmaviy |
| Tashkiliy, huquqiy va dasturiy |
| Huquqiy, texnologik va dasturiy |

**№ 60.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Loyihalashdagi xatoliklar va ma’muriy xatoliklar zaiflikni qaysi turiga mansub? |
| Texnologik |
| Texnik |
| Tashkiliy |
| Dasturiy |

**№ 61.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Mumkin bo'lgan hodisadan keyin tizimni asl holatiga qaytarish xarajatlarini hisobga olgan holda hisoblanadigan yo'qotish nima deb ataladi? |
| Zarar |
| Foyda |
| Oqibat |
| Sabab |

**№ 62.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Axborot xavfsizligi buzilishi natijasida tashkilotga yetkazilgan zararni sifat bo'yicha baholashda baholashning nechta darajasi tavsiya etiladi? |
| 3 |
| 4 |
| 5 |
| 2 |

**№ 63.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Zararni baholashda nechta me’zondan foydalanish taklif etiladi? |
| 4 |
| 5 |
| 3 |
| 2 |

**№ 64.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Axborot xavfsizligi buzilishidan kelib chiqadigan moddiy zarar qanday turdagi zarar hisoblanadi? |
| to'g'ridan-to'g'ri zarar |
| boshqa turdagi yo'qotishlar |
| yuzaga kelgan tahdidni zararsizlantirish uchun sarflangan xarajatlar |
| axborot xavfsizligi buzilganidan keyin tiklanish xarajatlari |

**№ 65.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Nufuzga putur yetishi, ishbilarmonlik aloqalarini uzish, tashkilot imidjini yaxshilash uchun qo'shimcha xarajatlar va boshqalar qaysi turdagi zararga kiradi? |
| Boshqa turdagi yo'qotishlar |
| To'g'ridan-to'g'ri zarar |
| Yuzaga kelgan tahdidni zararsizlantirish uchun sarflangan xarajatlar |
| Axborot xavfsizligi buzilganidan keyin tiklanish xarajatlari |

**№ 66.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| Administrator bayonnomas, rahbar xulosasi |
| Axborot xavfsizligi xodimlari hisoboti |
| Axborot texnologiyalari markazi rahbari hisoboti |

**№ 67.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Qachon tahdidlarni amalga oshirish ehtimoli dargumon deb hisoblanadi? |
| Agar tahdidni amalga oshirish uchun ob'ektiv shartlar mavjud bo'lmasa |
| Tahdidning yuzaga kelishi uchun ob'ektiv shartlar mavjud bo'lganda |
| Xavf amalga oshishining ob'ektiv old shartlari mavjud bo'lganda, lekin amalga oshirilayotgan xavfsizlik choralari yetarli bo'lmagan taqdirda |
| Tahdidning yuzaga kelishi uchun ob'ektiv shartlar mavjud bo'lganda va xavfsizlik choralari ko'rilmaganda |

**№ 68.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Qachon tahdidlarni amalga oshirish ehtimoli past deb hisoblanadi? |
| Tahdidning yuzaga kelishi uchun ob'ektiv shartlar mavjud bo'lganda |
| Agar tahdidni amalga oshirish uchun ob'ektiv shartlar mavjud bo'lmasa |
| Xavf amalga oshishining ob'ektiv old shartlari mavjud bo'lganda, lekin amalga oshirilayotgan xavfsizlik choralari yetarli bo'lmagan taqdirda |
| Tahdidning yuzaga kelishi uchun ob'ektiv shartlar mavjud bo'lganda va xavfsizlik choralari ko'rilmaganda |

**№ 69.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| Tahdidning yuzaga kelishi uchun ob'ektiv shartlar mavjud bo'lganda |
| Agar tahdidni amalga oshirish uchun ob'ektiv shartlar mavjud bo'lmasa |
| Tahdidning yuzaga kelishi uchun ob'ektiv shartlar mavjud bo'lganda va xavfsizlik choralari ko'rilmaganda |

**№ 70.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Qachon tahdidlarni amalga oshirish ehtimoli yuqori deb hisoblanadi? |
| Tahdidning yuzaga kelishi uchun ob'ektiv shartlar mavjud bo'lganda va xavfsizlik choralari ko'rilmaganda |
| Xavf amalga oshishining ob'ektiv old shartlari mavjud bo'lganda, lekin amalga oshirilayotgan xavfsizlik choralari yetarli bo'lmagan taqdirda |
| Tahdidning yuzaga kelishi uchun ob'ektiv shartlar mavjud bo'lganda |
| Agar tahdidni amalga oshirish uchun ob'ektiv shartlar mavjud bo'lmasa |

**№ 71.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Tahdid kattalilik darjasi |
| Riskni hajmi |
| Aktiv qiymati |

**№ 72.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo’yicha asosiy tushunchalar, fanning maqsadi va vazifalari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Zarar va hujum ehtimolini ko’paytmasining natijasi nimani beradi? |
| Risk |
| Zaiflik miqdori |
| Tahdidni amalga oshirilishi |
| Risk darajasi |

**№ 73.**

**Manba: 7-Ma‘ruza. AX risklarini qayta ishlash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Xavfdan qochish uchun biznes usullarini o'zgartiradigan har qanday harakatlar nima deb ataladi? |
| Riskdan qochish |
| Xavfni uzatish |
| Xavfni kamaytirish |
| Xavfni qabul qilish |

**№ 74.**

**Manba: 7-Ma‘ruza. AX risklarini qayta ishlash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Boshqalarning xavf va zararlar uchun javobgarlikni o'z zimmasiga olishi nima deyiladi? |
| Riskni uzatish |
| Xavfdan qochish |
| Xavfni kamaytirish |
| Xavfni qabul qilish |

**№ 75.**

**Manba: 7-Ma‘ruza. AX risklarini qayta ishlash**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Yo'qotish ehtimoli va hajmini kamaytirish nima deb ataladi? |
| Riskni kamaytirish |
| Xavfni uzatish |
| Xavfdan qochish |
| Xavfni qabul qilish |

**№ 76.**

**Manba: 7-Ma‘ruza. AX risklarini qayta ishlash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Xavfga qarshi choralar natijasida riskning boshlang'ich yoki maqbul qiymatini qabul qilinishiga nima deyiladi? |
| Riskni qabul qilish |
| Xavfni kamaytirish |
| Xavfni uzatish |
| Xavfdan qochish |

**№ 77.**

**Manba: 7-Ma‘ruza. AX risklarini qayta ishlash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Xavfni qabul qilish |
| Xavfni uzatish |
| Xavfdan qochish |

**№ 78.**

**Manba: 7-Ma‘ruza. AX risklarini qayta ishlash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Tashkilotning axborot xavfsizligini ta'minlash darajasini baholashda tashkilotdagi axborot xavfsizligi darajasiga bog'liq bo'lgan nechta parametr hisobga olinadi? |
| 3 |
| 4 |
| 5 |
| 2 |

**№ 79.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Har qanday qimmatli ma’lumotlar, qurilma yoki tashkilot tizimlarining boshqa komponentalari nima deb ataladi? |
| Aktiv |
| Tahdid manbalari |
| Axborot manabalari |
| Zaiflik |

**№ 80.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Qaysi standartda joriy qilishda tashkilotlarning bajarishi kerak bo’lgan birinchi narsa bu axborot aktivini aniqlash deb ko‘rsatilgan? |
| ISO 27001 |
| ISO 27000 |
| ISO 27004 |
| ISO 27005 |

**№ 81.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Muallif |
| huquq egasi |
| ishlab chiqaruvchi |

**№ 82.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Sabablar, oqibatlar, ta'sirlar, xavf zonalari va hodisalar to'g'risida olingan ma'lumotlarga asoslangan xavf-xatar bayonoti nima deb ataladi? |
| Oddiy spetsifikatsiya |
| Bazaviy identifikatsiya |
| Batafsil identifikatsiya |
| Autentifikatsiya |

**№ 83.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| …. - 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 |
| oddiy spetsifikatsiya |
| batafsil identifikatsiya |
| Autentifikatsiya |

**№ 84.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| bazaviy identifikatsiya |
| oddiy spetsifikatsiya |
| Autentifikatsiya |

**№ 85.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Bunda xatarlar ishning tegishli qismlari bilan taqqoslanadi. Gap qaysi jarayon haqida ketmoqda? |
| ichki o’zaro tekshiruv |
| Tashqi tekshiruv |
| Loyihalarni boshqarish |
| Hujjatlarni tahlil qilish |

**№ 86.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Dasturiy ta’minot, biznes ilovalar va tarmoq qanday turdagi aktivga kiradi? |
| yordamchi |
| asosiy |
| qo’shimcha |
| axborot |

**№ 87.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Insident sababli aktiv(lar) tomonidan ko'rsatiladigan xizmat tiklangunga qadar jarayondagi to'xtalishlar qiymati parametri ta’sirni baholashni qaysi turiga kiradi? |
| Bevosita |
| Bilvosita |
| Tashqi |
| Ichki |

**№ 88.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Xavfsizlikni buzish natijasida olingan ma'lumotlardan noto'g'ri foydalanish tas’irni baholashni qasyi turiga mansub? |
| Bilvosita |
| Bevosita |
| Tashqi |
| Ichki |

**№ 89.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Identifikatsiya jarayonini amalga oshirishning eng muvaffaqiyatli algoritmida birinchi qadam qanday? |
| Potensial risklarni aniqlash |
| Xatarlarni bartaraf etish usullarini aniqlash |
| Xavflarning oldini olish strategiyasini aniqlash |
| Xavflarni lokalizatsiya qilish strategiyasini aniqlash |

**№ 90.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Identifikatsiya jarayonini amalga oshirishning eng muvaffaqiyatli algoritmi nechta qadamdan iborat? |
| 6 |
| 5 |
| 7 |
| 4 |

**№ 91.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Aktivlarni chuqur aniqlash va baholashni, ushbu aktivlarga nisbatan tahdidlarni va zaifliklarni baholashni o'z ichiga oladigan jarayon bu qaysi? |
| Axborot xavfsizligi riskini batafsil baholash |
| Risklarni qisman baholash |
| Risklarni umumiy baholash |
| Tahdidlarni umumiy baholash |

**№ 92.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Axborot xavfsizligi riskini batafsil baholashning yakuniy bosqichi – bu qaysi? |
| Riskning umumiy bahosi |
| Axborot xavfsizligi xavfini batafsil baholash |
| Risklarni qisman baholash |
| Tahdid darajasi |

**№ 93.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Aktivlarni qayta shakllantirishdagi qulaylik, personal tomonidan yuzaga keluvchi tahdidlar ko'rib chiqilganda zaiflik hisobiga maqsadga erishish omili nimaga ta’sir qiladi? |
| Muayyan tahdid ehtimolligiga |
| Risk darajasi |
| Aktiv qiymati |
| Tahdidlar intensivligi |

**№ 94.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Amaliy risk boshqaruvi nechta jarayonni o’z ichiga oladi? |
| 4 |
| 3 |
| 5 |
| 6 |

**№ 95.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Bu yondashuv ko'pchilik xalqaro va rus standartlari va qoidalari nuqtai nazaridan afzaldir. Gap qaysi yondashuv haqida ketmoqda? |
| Belgilangan metodika bo'yicha rasmiy baholash |
| Qabul qilingan standartlar / modellardan foydalanish |
| Ekspertlar guruhining bahosi |
| Norasmiy/intuitiv baholash |

**№ 96.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Belgilangan metodika bo'yicha rasmiy baholash |
| Qabul qilingan standartlar / modellardan foydalanish |
| Norasmiy/intuitiv baholash |

**№ 97.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Belgilangan metodika bo'yicha rasmiy baholash |
| Ekspertlar guruhining bahosi |
| Norasmiy/intuitiv baholash |

**№ 98.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Qabul qilingan standartlar/modellardan foydalanish |
| Belgilangan metodika bo'yicha rasmiy baholash |
| Ekspertlar guruhining bahosi |

**№ 99.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Aktivni ishlab chiqish, saqlash yoki almashtirish nuqtai nazaridan har bir axborot aktiviga investitsiya darajasi qaysi jarayon omili hisoblanadi? |
| Riskni yuqori darajali baholash |
| Axborot xavfsizligi xavfini batafsil baholash |
| Risklarni qisman baholash |
| Tahdid darajasi |

**№ 100.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Riskni yuqori darajali baholashni boshlashdan maqsad nima? |
| Biznes uzluksizligi bilan bog’liq rejalar bilan sinxronlashtirish |
| tahdidlar, zaifliklar, aktivlar va oqibatlarni tizimli tahlil qilish |
| Byudjet, nazorat va boshqaruvi |
| Eng muhim xavflarni hisobga olish |

**№ 101.**

**Manba: 7-Ma‘ruza. AX risklarini qayta ishlash**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Sug'urta risklarni boshqarish usullarining qaysi guruhiga kiradi? |
| xavflardan qochish usullari |
| xavflarni diversifikatsiya qilish usullari |
| xavflarni lokalizatsiya qilish usullari |
| riskni qoplash usullari |

**№ 102.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| CRAMM usuli doirasida avtomatlashtirilgan protseduralarni bajarish quyidagilardan qaysini o'z ichiga oladi? |
| Ketma-ket uchta bosqichni ajratish. |
| Ikki ketma-ket bosqichni ajratish. |
| To'rtta ketma-ket bosqichlarni ajratish. |
| Ketma-ket besh bosqichni ajratish |

**№ 103.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| Himoya tizimining qo'llaniladigan vositalarini tahlil qilish va xulosa chiqariladi |
| Davolanish usullarini tahlil qilish va xulosa chiqariladi |
| Himoya choralarini tahlil qilish va xulosa chiqariladi |

**№ 104.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| CRAMM usuli doirasida, agar resurslarning kritik darajasi juda past bo'lsa, tizimga qanday xavfsizlik talablari qo‘yiladi? |
| Tizimga minimal xavfsizlik talablari quyiladi |
| Tizimga xavfsizlik talablarining maksimal to'plami qo'yiladi |
| Tizimda o'rtacha xavfsizlik talablari mavjud |
| Tizim uchun xavfsizlik talablari yo'q |

**№ 105.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| CRAMM usuli doirasida ikkinchi bosqichda nimalar bajariladi? |
| Xavfsizlik tahdidlari va zaifliklari tahlili amalga oshirish |
| Xavfsizlik tahdidlari tahlili olib borish |
| Tahdidlar oqibatlarini tahlil qilish |
| Aktiv qiymatini tahlil qilish |

**№ 106.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| CRAMM usuli doirasida uchinchi bosqichda nimalar bajariladi? |
| Risklarni boshqarish muammosi hal qilinadi, tegishli qarshi choralar tanlash |
| Xatarlarni boshqarish muammosi hal qilish |
| Tegishli qarshi choralarni tanlash |
| Yangi qarshi choralarni amalga oshirish rejasini tayyorlash |

**№ 107.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| CRAMM ning qarshi choralar uchun bir nechta variantlarni avtomatik ravishda yaratish imkoniyatini belgilang. |
| 1000 dan ortiq |
| 1500 dan ortiq |
| 2000 dan ortiq |
| 10000 dan ortiq |

**№ 108.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| Yaxshi tuzilgan |
| Keng sinovdan o'tgan usul |
| Dasturiy ta'minot mahsuloti qarshi choralar bo'yicha etarlicha katta bilimlar bazasiga asoslangan |

**№ 109.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| CRAMM usulining kamchiliklari keltirilgan javobni belgilang. |
| Maxsus tayyorgarlik va yuqori malakani talab qiladi |
| Maxsus tayyorgarlik va yuqori malakani talab qilmaydi |
| Yuqori malaka talab qilmaydi |
| Yuqori malaka talab qiladi |

**№ 110.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| Xodimlarning sog'lig'iga zarar yetkazish |
| Majburiyatlarni bajara olmaslik bilan bog'liq yo'qotishlar |
| Faoliyatning tartibsizligi |

**№ 111.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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) |
| To'g'ridan-to'g'ri zarar, bilvosita zarar |
| Qayta tiklash bilan bog'liq zarar |
| Investitsiyalar rentabelligini (ROI) baholash |

**№ 112.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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) |
| Yo'qotishlarning tashkilotga ta'siri - tashkilot faoliyatining bir jihati |
| Ma'lumotlarni uzatish tarmog'i orqali harakat qiluvchi buzg'unchi tomonidan yuzaga keladigan tahdidlar |
| Tashkilot ichida harakat qiluvchi buzg'unchi tomonidan tahdidlar |

**№ 113.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| RiskWatch usuli doirasida avtomatlashtirilgan protseduralarni bajarish quyidagilardan qaysi birini o'z ichiga oladi? |
| To'rtta ketma-ket bosqichlarni ajratish. |
| Ketma-ket uchta bosqichni ajratish. |
| Ikki ketma-ket bosqichni ajratish. |
| Ketma-ket besh bosqichni ajratish |

**№ 114.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| RiskWatch usuli doirasida birinchi bosqichda nima amalga oshiriladi? |
| Tadqiqot predmetining ta'rifi. Tashkilot turi, o'rganilayotgan tizimning tarkibi (umumiy ma'noda), bazaviy xavfsizlik talablari |
| Himoya tizimining qo'llaniladigan vositalarini tahlil qilish |
| Asosiy xavfsizlik talablari |
| Yuqori darajadagi xavfsizlik talablari |

**№ 115.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| Tizimning o'ziga xos xususiyatlarini tavsiflovchi ma'lumotlarni kiritish. resurslar, yo'qotishlar va hodisalar sinflari aniqlash |
| Tizimning o'ziga xos xususiyatlarini tavsiflovchi ma'lumotlarni kiritish |
| Resurslarni baholash, yo'qotish va hodisalar sinflari aniqlash |

**№ 116.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| RiskWatch usuli doirasida uchinchi bosqichda nima amalga oshiriladi? |
| Xavfni miqdoriy baholash |
| Xavfni sifat va miqdoriy baholash |
| Xavfni sifatli baholash |
| Yillik yo'qotishlarni hisoblash |

**№ 117.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| RiskWatch usuli doirasida to‘rtinchi bosqichda qanday ish amalga oshiriladi? |
| Hisobotlarni yaratish |
| Tavsiya yaratish |
| Oqibatlarni keltirib chiqarish |
| Tavsiyalar va natijalarni ishlab chiqish |

**№ 118.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Quyidagi keng tarqalgan risklarni tahlil qilish usullaridan qaysi biri xavfni sifat jihatidan baholash usulidan foydalanadi (masalan, “yuqori”, “o‘rta”, “past” shkalasi bo‘yicha)? |
| CRAMM |
| FRAP |
| RiskWatch |
| Octave |

**№ 119.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Xavf omillarini kuzatish va qayta ko'rib chiqish uchun qanday kirish ma'lumotlaridan foydalaniladi? |
| Risklarni boshqarish harakatlari natijasida olingan risklar haqidagi barcha ma'lumotlar |
| Aniqlangan xavflar ro'yxati |
| Tahdidlarning oqibatlari ro'yxat |
| Tahdidlar va zaifliklar ro'yxati |

**№ 120.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| Xatarlarni boshqarishni tashkilotning biznes maqsadlari va risklarni qabul qilish mezonlari bilan doimiy ravishda muvofiqlashtirish |
| Xatarlarni boshqarishni baholash |
| Aniqlangan xavflar |

**№ 121.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| Xatarlar statik bo'lib qolmoqda |
| Xatarlar statik bo'lib qolmaydi |
| Tahdidlar, zaifliklar, ehtimolligi yoki oqibatlar o'zgarmaydi |

**№ 122.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Tashkilotlar qanday omillarning doimiy monitoringini ta'minlashi lozim deyiladi? |
| Xatarlarni boshqarish doirasiga kiritilgan yangi aktivlarni |
| Aktivlar qiymatini o'zgartirish talabi yo'q, masalan, biznesning qulay talablari tufayli |
| Tashkilot tashqarisida va ichida faol bo'lmasligi mumkin bo'lgan tahdidlar allaqachon baholangan |
| Zaifliklarning kamayishi ehtimoli tahdidlarga ushbu yangi yoki o'zgartirilgan zaifliklardan foydalanishga imkon berishi mumkin |

**№ 123.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Tashkilotlar qanday omillarning doimiy monitoringini ta'minlashi lozim? |
| Tashkilot tashqarisida va ichida faol bo'lishi mumkin bo'lgan hali baholanmagan yangi tahdidlar |
| risklarni boshqarish doirasiga kiritilmagan aktivlar; |
| Aktivlar qiymatini o'zgartirish talabi yo'q, masalan, biznesning qulay talablari tufayli |
| Zaifliklarning kamayishi ehtimoli tahdidlarga ushbu yangi yoki o'zgartirilgan zaifliklardan foydalanishga imkon berishi mumkin. |

**№ 124.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Tashkilotlar qanday omillarning doimiy monitoringini olib borishi talab etiladi? |
| Yangi yoki kuchaygan zaifliklarning tahdidlarga ushbu yangi yoki o'zgartirilgan zaifliklardan foydalanishga imkon berishi ehtimolini |
| risklarni boshqarish doirasiga kiritilmagan aktivlar |
| Aktivlar qiymatini o'zgartirish talabi yo'q, masalan, biznesning qulay talablari tufayli |
| Tashkilot tashqarisida va ichida faol bo'lmasligi mumkin bo'lgan tahdidlar allaqachon baholangan. |

**№ 125.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 1**

|  |
| --- |
| 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 |
| Huquqiy kontekst, raqobat konteksti |
| Ta'sir mezonlari, xavfni baholash mezonlari |
| Aktivlarni ishlatishning to'liq qiymati |

**№ 126.**

**Manba: 7-Ma‘ruza. AX risklarini qayta ishlash**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Potensial xavfni kamaytirish strategiyalari nimani ichiga oladi? |
| Riskni kamaytirish |
| Xavfni yashirish |
| Xavfli reklama |
| Xavf nominatsiyasi |

**№ 127.**

**Manba: 7-Ma‘ruza. AX risklarini qayta ishlash**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Potensial xavfni kamaytirish strategiyalari nimani ichiga oladi? |
| Riskni sug'urtalashni |
| Xavf nominatsiyasi |
| Xavfning parchalanishi |
| Xavfni yashirish |

**№ 128.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Risklarni boshqarish bosqichlaridan biri bu qaysi? |
| Aktivlarni identifikatsiya qilish |
| Majburiyatlarni tugatish |
| Tahlil qilinadigan ob'ektlarni tanlash |
| Zaifliklarni aniqlash |

**№ 129.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Quyidagilardan qaysi biri risklarni boshqarish bosqichlariga tegishli? |
| Tahdid tahlili |
| Tahdidlarni yo'q qilish |
| Zaifliklarni aniqlash |
| Zaifliklarni yaratish uchun jazoaifliklarni yaratish uchun jazolash |

**№ 130.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Tahdidlarni tahlil qilishning birinchi bosqichini belgilang? |
| Tahdidlarni identifikasiyalash |
| Tahdid autentifikatsiyasi |
| Tahdidlarni yo'q qilish |
| Zaifliklarni aniqlash |

**№ 131.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 1**

|  |
| --- |
| Xatarlarni baholash qanday savollarga javob berishga imkon beradi? |
| Mavjud xavflar qabul qilinadimi |
| Xatarlar qabul qilib bo'lmaydigan bo'lsa, kim aybdor |
| Xatarlarni maqbul qilish uchun nima qilish kerak |
| Axborot tizimi foydalanuvchilari uchun qanday xavflar mavjud |

**№ 132.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 27000 oilasiga mansub xalqaro standartlar asosida qabul qilingan Axborot xavfsizligiga oid standartlar soni nechta? |
| 5 |
| 10 |
| 15 |
| 20 |

**№ 133.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| O'z DSt ISO / IEC 27001: 2009 standarti nimani belgilaydi? |
| Axborot xavfsizligini boshqarish tizimlari. Talablarni. |
| Axborot xavfsizligini boshqarishning amaliy qoidalari |
| Axborot xavfsizligini boshqarish tizimini joriy qilish bo'yicha qo'llanma |
| Axborot xavfsizligini boshqarish tizimining samaradorligini o'lchash |

**№ 134.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| O'z DSt ISO / IEC 27002: 2008 standarti nimani belgilaydi? |
| Axborot xavfsizligini boshqarishning amaliy qoidalarini |
| Axborot xavfsizligini boshqarish tizimlari. Talablar. |
| Axborot xavfsizligini boshqarish tizimini joriy qilish bo'yicha qo'llanma |
| Axborot xavfsizligini boshqarish tizimining samaradorligini o'lchash |

**№ 135.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| O'z DSt ISO / IEC 27003: 2014 standarti nimani belgilaydi? |
| Axborot xavfsizligini boshqarish tizimini joriy qilish bo'yicha qo'llanmani |
| Axborot xavfsizligini boshqarish tizimining samaradorligini o'lchash |
| Axborot xavfsizligini boshqarishning amaliy qoidalari |
| Axborot xavfsizligini boshqarish tizimlari. Talablar |

**№ 136.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| O'z DSt ISO / IEC 27004: 2014 standarti nimani belgilaydi? |
| Axborot xavfsizligini boshqarish tizimining samaradorligini o'lchashni |
| Axborot xavfsizligini boshqarishning amaliy qoidalari |
| Axborot xavfsizligini boshqarish tizimlari. Talablar. |
| Axborot xavfsizligini boshqarish tizimini joriy qilish bo'yicha qo'llanma |

**№ 137.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| O'z DSt ISO / IEC 27005: 2016 standarti nimani belgilaydi? |
| Axborot xavfsizligi risklarini boshqarishni |
| Axborot xavfsizligini boshqarish tizimining samaradorligini o'lchash |
| Axborot xavfsizligini boshqarishning amaliy qoidalari |
| Axborot xavfsizligini boshqarish tizimlari. Talablar |

**№ 138.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| O'z DSt ISO / IEC 27005: 2016 bo'yicha xavf tahlili deganda nima tushuniladi? |
| Tavakkalchilikning mohiyatini tushunish va xavf darajasini aniqlash jarayoni. |
| Riskni tushunish jarayoni va xavfni aniqlash |
| Xavfning mohiyatini tushunish va tahdidni aniqlash jarayoni |
| Xavfning mohiyatini tushunish va zaiflikni aniqlash jarayoni |

**№ 139.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| O'z DSt ISO / IEC 27005: 2016 bo'yicha xavf mezoni nima? |
| Xatarning ahamiyatliligi bilan baholanadigan qoidalar |
| Xatarlarni aniqlash qoidalari |
| Tahdidni aniqlash qoidalari |
| Zaiflikni aniqlash qoidalari |

**№ 140.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| O'z DSt ISO / IEC 27005: 2016 bo'yicha riskni qayta ishlash nima? |
| Xavfni o'zgartirish jarayoni |
| Xavflarni qidirish jarayoni |
| Xavfni e'tiborsiz qoldirish jarayoni |
| Risklarni boshqarish jarayoni |

**№ 141.**

**Manba: 11-Ma‘ruza. Risklarni boshqarish sohasiga oid xalqaro va milliy standartlar**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| Xatarlarni tahlil qilish natijalarini taqqoslash jarayoni |
| Axborot xavfsizligi xavfini baholash natijalarini taqqoslash jarayoni |
| Xatarlarni tahlil qilish natijalarini axborot xavfsizligi bilan solishtirish jarayoni |

**№ 142.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo’yicha asosiy tushunchalar, fanning maqsadi va vazifalari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Axborot xavfsizligi xavfi deganda nima tushuniladi? |
| Tahdidlarni amalga oshirishda axborot aktivlari yoki axborot aktivlari guruhining zaifligidan foydalangan holda tashkilotga yetkazilgan zarar |
| Aktivning ahamiyatini buzish |
| Aktiv qiymatining o'zgarishi |
| Aktivning zaifligining kattaligi |

**№ 143.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo’yicha asosiy tushunchalar, fanning maqsadi va vazifalari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| Tashkilotning xavfsizlik darajasini baholash |
| Xatarlarni boshqarishga yondashuvni o'zgartirish uchun ma'lumot to'plash |
| Xatarlarni davolashning doimiy monitoringi samaradorligini pasaytirish |

**№ 144.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Axborot xavfsizligi risklarini boshqarish jarayoni qanday bosqichlardan iborat? |
| Kontekstni aniqlash, xavfni aniqlash, xavfni tahlil qilish, xavfni baholash, xavfni qayta ishlash |
| Kontekstni aniqlash, ma'lumotlar almashinuvi va maslahat |
| Aktivlarni identifikatsiya qilish, xavf tahlili |
| Tahdidlarni aniqlash, kontekstni o'rnatish |

**№ 145.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Axborot xavfsizligini boshqarish tizimi qanday bosqichlardan iborat? |
| Rejalashtirish, amalga oshirish, tekshirish, harakat qilish |
| Rejalashtirish, o'zgartirish, sozlash |
| O'zgartirish, sozlash, harakat |
| Moslashtirish, rejalashtirish, amalga oshirish |

**№ 146.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Xatarlarni qabul qilish mezonlari nima asosidabelgilanadi? |
| Biznes mezonlari, qonunchilik va tartibga solish jihatlari, operatsiyalar, texnologiya, moliya, ijtimoiy va gumanitar omillar |
| Moliyaviy, ijtimoiy va gumanitar omillar |
| Qonunchilik va me'yoriy-huquqiy hujjatlar |
| Operatsiyalar, texnologiya, moliya |

**№ 147. 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Manba:**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Tashkilotning axborot xavfsizligini boshqarish darajalarini belgilang? |
| Strategik boshqaruv, taktik boshqaruv, operativ boshqaruv |
| Uzoq muddatli rejalashtirish, qisqa muddatli nazorat, taktik nazorat |
| Strategik boshqaruv, uzoq muddatli rejalashtirish, qisqa muddatli boshqaruv |
| Operatsion boshqaruv, tor rejalashtirish, maxsus rejalashtirish |

**№ 148.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Strategik boshqaruv darajasining funksional komponentlari qaysilar? |
| Tashkilotning texnik siyosatini, axborot xavfsizligi xizmatini, huquqiy nazoratni ta'minlash |
| Xizmat ko'rsatish, huquqiy nazorat, aloqa |
| Maxsus ma'muriyat, qoida yaratish nazorati |
| Global nazorat, mahalliy nazorat |

**№ 149.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Taktik rejalashtirish darajasining funksional komponentlarini belgilang. |
| Axborot xavfsizligi siyosatini shakllantirish, nazorat qilish, tahlil qilish, ekspertiza, tekshirish. |
| Sinov operatsiyasi, nazorat qilish |
| tahlil qilish, tekshirish, tekshirish |
| Sinov operatsiyasi, nazorat, tergov |

**№ 150.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Operativ rejalashtirish darajasining funksional komponentlarini belgilang. |
| Monitoring, maxsus himoya vositalarini nazorat qilish, nazorat qilish, boshqarish, avtomatlashtirilgan tizim vositalarini boshqarish. |
| Maxsus himoya vositalarini amalga oshirish, boshqarish |
| Operatsiya, chora izlash |
| Yaxshilash, javob berish vositalari |

**№ 151.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Tashkilotda axborot xavfsizligini boshqarish komponentlarini belgilang. |
| AX boshqaruv jarayonining o'zi va tashkilotning AX boshqaruv tizimi (AXBT). |
| Strategik boshqaruv, qisqa muddatli boshqaruv. |
| Uzoq muddatli rejalashtirish, qisqa muddatli boshqaruv. |
| Strategik boshqaruv, uzoq muddatli rejalashtirish, qisqa muddatli boshqaruv. |

**№ 152.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Axborot xavfsizligini boshqarish tizimining uslubiy asosi to‘g‘ri ko’rsatilgan qatorni toping? |
| Axborot xavfsizligini boshqarish doirasidagi jarayonli yondashuv |
| Axborot xavfsizligini boshqarishda blokli yondashuv |
| Axborot xavfsizligini boshqarish doirasidagi tizimli yondashuv |
| Axborot xavfsizligi risklarini boshqarish doirasidagi yuqori darajadagi yondashuv |

**№ 153.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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 |
| Tashkilotning axborot xavfsizligini buzish xavfini minimallashtirishning eng to'g'ri va samarali usuli |
| Axborot xavfsizligini boshqarish doirasidagi tizimli yondashuv |
| Axborot xavfsizligi risklarini boshqarish doirasidagi yuqori darajadagi yondashuv |

**№ 154.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi –**

|  |
| --- |
| 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 |
| Integratsiyalashgan, tuzilgan va murakkab |
| murakkab, keng qamrovli. |
| dinamik, barcha mavjud ma'lumotlar |

**№ 155.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Risklarni boshqarishda “integratsiyalashgan” tamoyilini to‘g‘ri ochib beruvchi qatorni ajratib ko‘rsating. |
| Risklarni boshqarish har qanday tashkilot biznesining ajralmas qismidir |
| Risklarni boshqarish tashkilot faoliyatining ajralmas qismi emas |
| Risklarni boshqarish axborot xavfsizligining ajralmas qismi hisoblanadi |
| Xatarlarni boshqarish AKT tayyorligi |

**№ 156.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| risklarni boshqarish tuzilmasi va jarayoni ishlab chiqilgan va tashkilotning tashqi va ichki kontekstiga mos keladi |
| manfaatdor tomonlarni tegishli va o'z vaqtida jalb qilish |
| Xatarlar paydo bo'lishi, o'zgarishi yoki yo'qolishi mumkin |

**№ 157.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| 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. |
| manfaatdor tomonlarni tegishli va o'z vaqtida jalb qilish |
| Xatarlar paydo bo'lishi, o'zgarishi yoki yo'qolishi mumkin |
| Xatarlarni boshqarishga o'ylangan va tushunarli yondashuv |

**№ 158.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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. |
| Xatarlarni boshqarish bo'yicha dastlabki ma'lumotlar tarix va joriy ma'lumotlarga asoslanadi |
| Xatarlar paydo bo'lishi, o'zgarishi yoki yo'qolishi mumkin |
| Xatarlarni boshqarishga o'ylangan va tushunarli yondashuv |

**№ 159.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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. |
| Xatarlarni boshqarishga o'ylangan va to'g'ridan-to'g'ri yondashuv kamchiliklar va taqqoslanadigan natijalarni taqqoslashga qarshi turadi. |
| Xatarlarni boshqarish tuzilmasi va jarayoni ishlab chiqilgan va tashkilotning tashqi va ichki kontekstiga mos keladi |
| manfaatdor tomonlarni tegishli va o'z vaqtida jalb qilish |

**№ 160.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Xatarlarni boshqarishga o'ylangan va tushunarli yondashuv kamchiliklarga va taqqoslanadigan natijalarni taqqoslashga qarshi turadi |
| Xatarlarni boshqarish tuzilmasi va jarayoni ishlab chiqilgan va tashkilotning tashqi va ichki kontekstiga mos keladi |
| manfaatdor tomonlarni tegishli va o'z vaqtida jalb qilish |

**№ 161.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Xatarlarni boshqarishga o'ylangan va tushunarli yondashuv kamchiliklarni bartaraf qiladi va taqqoslanadigan natijalarni taqqoslaydi |
| risklarni boshqarish tuzilmasi va jarayoni ishlab chiqilgan va tashkilotning tashqi va ichki kontekstiga mos keladi |
| manfaatdor tomonlarni tegishli va o'z vaqtida jalb qilish |

**№ 162.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Risklarni boshqarishda “Doimiy takomillashtirish” tamoyilini to'g'ri ochib beruvchi qatorni ajratib ko'rsating |
| Risklarni boshqarish trening va tajriba orqali doimiy ravishda takomillashtiriladi |
| Inson xulq-atvori va madaniyati har bir daraja va bosqichda risklarni boshqarishning barcha jihatlariga sezilarli darajada ta'sir qiladi |
| Xatarlarni boshqarishga o'ylangan va tushunarli yondashuv kamchiliklarni bartaraf qiladi va taqqoslanadigan natijalarni taqqoslaydi |
| Risklarni boshqarish tuzilmasi va jarayoni ishlab chiqilgan va tashkilotning tashqi va ichki kontekstiga mos keladi |

**№ 163.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Korxona yoki tashkilot aktivlarining qiymatini baholash maqsadini belgilang. |
| aktiv ahamiyatini baholash va aktivlarni himoya qilishning zaruriy darajasini aniqlash |
| riskni uzatish |
| riskni qabul qilish |
| muvofiqlashtirish |

**№ 164.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Aktivlar nechta o'lchov asosida baholanadi? |
| 3 |
| 2 |
| 5 |
| 4 |

**№ 165.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Aktivlarni baholashning uch o'lchovi bu qaysilar? |
| Maxfiylik, yaxlitlik va mavjudlik |
| Uzatiluvchi, qabul qilinuvchi, qayta ishlanuvchi |
| Doimiy, vaqtincha, o’zgarmas |
| Sodda, murakkab, gibrid |

**№ 166.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Aktivlarni baholash usullarini belgilang. |
| sifat va miqdoriy baholash |
| miqdoriy baholash |
| sifat darajasi bo’yicha baholash |
| sodda, murakkab, gibrid |

**№ 167.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari Qiyinlik darajasi – 2**

|  |
| --- |
| Sifat darajasi bo'yicha baholashning darajalarini aniqlang. |
| Ahamiyatsiz, Past, O'rtacha, Yuqori, Halokatli |
| Ahamiyatsiz, Past, O'rtacha, Yuqori |
| Past, O'rtacha, Yuqori, Halokatli |
| sodda, murakkab, gibrid |

**№ 168.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Zaiflik tahlili mohiyatini aniqlang. |
| Tashkilotning mumkin bo'lgan zaif tomonlarini sanab o'tish va ularni "kuchliligi" ga qarab toifalarga ajratish |
| Axborot xavfsizligini boshqarish tizimini qo'llab-quvvatlash |
| Insidentlarga javob rejasini tayyorlash |
| Biznesning uzluksizligi rejasini tayyorlash |

**№ 169.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Zaifliklar toifalarini belgilang. |
| Texnik, texnologik, tashkiliy |
| Ahamiyatsiz, Past, O'rtacha, Yuqori |
| Past, O'rtacha, Yuqori, Halokatli |
| sodda, murakkab, gibrid |

**№ 170.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Loyihalashda xatolik, ma'muriy xato qaysi zaiflik toifasiga kiradi? |
| Texnologik |
| Texnik |
| Tashkiliy |
| murakkab |

**№ 171.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Aktivni sifat bo'yicha baholashda dastlabki xavfsizlik darajasi qachon “yuqori” deyiladi? |
| Agar aktivlarning kamida 70 foizi "yuqori" darajaga to'g'ri kelsa |
| Agar aktiv 1-band shartlarini bajarilmasa va uning xususiyatlarining kamida 70% i "o'rtacha" dan past bo'lmagan darajaga to'g'ri kelsa |
| 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 |
| Barcha aktivlar qimmatlilik darajasi teng bo’lsa |

**№ 172.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Agar aktivlarning kamida 70 foizi "yuqori" darajaga to'g'ri kelsa |
| 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 |
| Barcha aktivlar qimmatlilik darajasi teng bo’lsa |

**№ 173.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Agar aktiv 1-band shartlarini bajarilmasa va uning xususiyatlarining kamida 70% i "o'rtacha" dan past bo'lmagan darajaga to'g'ri kelsa |
| Agar aktivlarning kamida 70 foizi "yuqori" darajaga to'g'ri kelsa |
| Barcha aktivlar qimmatlilik darajasi teng bo’lsa |

**№ 174.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Axborot xavfsizligining xavflarini baholash tartibi qanday aniqlanadi? |
| Axborot xavfsizligiga qo‘yiladigan talablar xavflarni muntazam baholash yordamida aniqlanadi |
| Axborot xavfsizligini boshqarish bo‘yicha tadbirlarga ketgan sarf-xarajatlar yordamida aniqlanadi |
| Axborot xavfsizligiga qo‘yiladigan talablar xavflarni sarf-xarajatlar yordamida aniqlanadi |
| Axborot xavfsizligiga qo‘yiladigan talablar xavflarni sarf-xarajatlar yordamida aniqlanadi |

**№ 175.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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. |
| Axborot xavfsizligini boshqarish uchun amal qilinadigan prinsiplar sifatida qabul qilinishi va uni joriy qilish mumkin. |
| Axborot xavfsizligini boshqarish uchun amal qilinadigan prinsiplar sifatida qabul qilinishi tayanch nuqta bo‘lishi mumkin. |
| Axborot xavfsizligini boshqarish va qabul qilinishi va uni joriy qilish uchun tayanch nuqta bo‘lib xizmat qilishi mumkin. |

**№ 176.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| AXBT siyosati, metodlari, jarayonlari va protseduralarini joriy etish va uning ishlashi |
| Jarayonlarning AXBT siyosati va maqsadlariga muvofiqligini baholash va zarurat bo‘lganida samaradorligini o‘lchash |
| Natijalarning yuqori rahbariyat tomonidan tahlil qilinishi |

**№ 177.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Amalga oshirish (AXBTni joriy etish va uning ishlashi) deganda nimani tushunasiz? |
| AXBT siyosati, metodlari, jarayonlari va protseduralarini joriy etish va uning ishlashi |
| Jarayonlarning AXBT siyosati va maqsadlariga muvofiqligini baholash va zarurat bo‘lganida samaradorligini o‘lchash |
| Natijalarning yuqori rahbariyat tomonidan tahlil qilinish |
| AXBT ichki auditlari natijalariga, rahbariyat tomonidan qilingan tahlil yoki uzluksiz takomillashtirish maqsadida boshqa manbalardan olingan ma’lumotlarga asoslangan tuzatuvchi va ogohlantiruvchi harakatlarni bajarish |

**№ 178.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Tekshirish (AXBT monitoringi va tahlili) deganda nimani tushunasiz? |
| Jarayonlarning AXBT siyosati va maqsadlariga muvofiqligini baholash va zarurat bo‘lganida samaradorligini o‘lchash |
| Natijalarning yuqori rahbariyat tomonidan tahlil qilinishi |
| AXBT siyosati, metodlari, jarayonlari va protseduralarini joriy etish va uning ishlashiAXBT ichki auditlari natijalariga, rahbariyat tomonidan qilingan tahlil yoki uzluksiz takomillashtirish maqsadida boshqa manbalardan olingan ma’lumotlarga asoslangan tuzatuvchi va ogohlantiruvchi harakatlarni bajarish |
| 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 |

**№ 179.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| AXBT siyosati, metodlari, jarayonlari va protseduralarini joriy etish va uning ishlashi Jarayonlarning AXBT siyosati va maqsadlariga muvofiqligini baholash va zarurat bo‘lganida samaradorligini o‘lchash. |
| Natijalarning yuqori rahbariyat tomonidan tahlil qilinishi |
| 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 |

**№ 180.**

**Manba: 9-Ma‘ruza. Monitoring va risk faktorlarini qayta ko'rib chiqish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Jarayonlarning AXBT siyosati va maqsadlariga muvofiqligini baholash |
| Tashkilotning umumiy siyosati va maqsadlarida e’lon qilingan natijalarga erishish |
| xatarlarni identifikatsiya qilish |

**№ 181.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Tashkilotda xatarlarni baholashga yondashishni aniqlashda nima amalga oshiriladi? |
| AXBT uchun mos keladigan xatarlarni baholash uslubiyatini aniqlash, shuningdek, axborot xavfsizligi sohasida tashkilot faoliyatini ta’minlash |
| tashkilotdagi xatarlarni baholash mezonlarini belgilash |
| AXBT ishlab chiqiladigan va qo‘llab-quvvatlanadigan tashkilot miqyosida xatarlarni boshqarishning tanlangan strategiyasini ishlab chiqish |
| xatarlarni identifikatsiya qilish |

**№ 182.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Tashkilot AXBT hujjatlarining hajmi nimalarga bog‘liq? |
| Tashkilotning miqyosi va uning faoliyat turi, boshqaruv amalga oshiriladigan tizim xavfsizligi talablarining qo‘llanish sohasi va murakkabliligi |
| Ishchilar soniga |
| Raxbariyatga |
| Ro‘yxatga olish yozuvlariga |

**№ 183.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Biznesning boshqa muhim aktivlari kabi qiymatga ega bo‘lgan aktiv nima? |
| Axborot |
| Konsepsiya |
| Ilova |
| Xujjat |

**№ 184.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Axborotni biznesning uzluksizligini ta’minlash |
| Xavflarini minimumga keltirish |
| Biznes imkoniyatlarini maksimal oshirish |

**№ 185.**

**Manba: 5-Ma‘ruza. Risklarni tahlil qilish bosqichlari**

**Qiyinlik darajasi – 3**

|  |
| --- |
| AXB ning bazaviy jarayonlari nima? |
| Axborot xavfsizligi risklarini boshqarish, axborot xavfsizligi insidentlarini boshqarish |
| Axborot xavfsizligi risklarini boshqarish, Biznesning uzluksizligini boshqarish |
| Biznesning uzluksizligini boshqarish, axborot xavfsizligi hodisalarini boshqaris |
| Axborot xavfsizligi inqirozi hodisalarini boshqarish |

**№ 186.**

**Manba: 12-Ma‘ruza. Biznesning uzluksizligini boshqarish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Biznes uzluksizligini boshqarish kompleks boshqaruv jarayoni sifatida nimani o'z ichiga oladi? |
| Tashkilotning ishida buzilishlar aniqlangan taqdirda tiklanish yoki uning faoliyatini davom ettirishni boshqarish |
| Tashkilotning biznes maqsadlariga mos kelmaydigan uzilishlar ta'sirini hisobga olish. |
| Axborotni qayta ishlash vositalari va usullarini tanlash |
| Hodisaga asoslangan uzilishlarning ta'sirini tushunish |

**№ 187.**

**Manba: 12-Ma‘ruza. Biznesning uzluksizligini boshqarish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Biznes uzluksizligini boshqarish jarayonini nechta yo‘nalishga bo'lish mumkin? |
| Biznes jarayonlarining insidentlarga chidamliligini ta'minlash, tashkilotning biznesini tiklash |
| Tashkilotning biznes maqsadlariga mos kelmaydigan uzilishlar ta'sirini hisobga olish. |
| Axborotni qayta ishlash vositalari va usullarini tanlash |
| Hodisaga asoslangan uzilishlarning ta'sirini tushunish |

**№ 188.**

**Manba: 12-Ma‘ruza. Biznesning uzluksizligini boshqarish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Biznes jarayonlarining insidentlarga chidamliligini ta’minlashdan maqsad nima? |
| Xavfli hodisaning yuzaga kelish ehtimolini kamaytirishda va inqirozga qarshi profilaktika choralarini ishlab chiqish va amalga oshirish |
| Tashkilotning biznes maqsadlariga mos kelmaydigan uzilishlar ta'sirini hisobga olish |
| Axborotni qayta ishlash vositalari va usullarini tanlash |
| Insidentlarga asoslangan uzilishlarning ta'sirini tushunish |

**№ 189.**

**Manba: 12-Ma‘ruza. Biznesning uzluksizligini boshqarish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Biznes faoliyatni tiklanishini ta’minlash nimadan iborat? |
| Oldindan sodir bo'lgan hodisaning salbiy ta'sirini kamaytirish va tuzatish |
| Sodir bo'lgan hodisani ta'sirini tuzatish |
| Voqea sodir bo'lmagan hodisaning salbiy ta'sirini maksimal darajada oshirish va tuzatish |
| Oldindan sodir bo'lgan hodisaning salbiy ta'sirini o'rtacha hisoblash |

**№ 190.**

**Manba: 12-Ma‘ruza. Biznesning uzluksizligini boshqarish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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 |
| Tashkilotning biznes maqsadlariga mos kelmaydigan uzilishlar ta'sirini hisobga olish |
| Axborotni qayta ishlash vositalari va usullarini tanlash |
| Hodisaga asoslangan uzilishlarning ta'sirini tushunish |

**№ 191.**

**Manba: 12-Ma‘ruza. Biznesning uzluksizligini boshqarish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Biznes uzluksizligini boshqarish jarayonining ikkinchi asosiy jihati keltirilgan qatorni ajratib ko'rsating. |
| Muhim biznes jarayonlarida ishtirok etadigan barcha aktivlarni aniqlash |
| Tashkilotning biznes maqsadlariga mos kelmaydigan uzilishlar ta'sirini hisobga olish |
| Axborotni qayta ishlash vositalari va usullarini tanlash |
| Hodisaga asoslangan uzilishlarning ta'sirini tushunish |

**№ 192.**

**Manba: 12-Ma‘ruza. Biznesning uzluksizligini boshqarish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| 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. |
| Axborotni qayta ishlash vositalari va usullarini tanlash |
| Hodisaga asoslangan uzilishlarning ta'sirini tushunish |
| Biznes jarayonlarida ishtirok etuvchi barcha aktivlarni aniqlash |

**№ 193.**

**Manba: 6 - Ma‘ruza. Riskni sifat va miqdor ko‘rsatkichini baholash**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Tahdid aniqlanganidan keyingi baholanuvchi jarayon bu qaysi? |
| Uni amalga oshirish ehtimolini |
| Uni amalga oshirishdagi yo'qotishlar |
| Uni amalga oshirish chastotasi |
| Investitsiyalar hajmi |

**№ 194.**

**Manba: 4 - Ma‘ruza. Aktivlarni identifikatsiya qilish**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Himoya choralari narxini tahlil qilishda e'tiborga olinuvchi jihatlarni belgilang. |
| Uskunalar sotib olish xarajatlarini |
| Dasturni sotib olish xarajatlarini |
| Kadrlar tayyorlash xarajatlarini |
| Kadrlarni qayta tayyorlash xarajatlarini |

**№ 195.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Risk tahdiddan nimasi bilan farqlanadi? |
| Mumkin bo'lgan yo'qotishlarni miqdoriy baholash va (ehtimol) tahdidning amalga oshishi ehtimolini baholashning mavjudligi bilan |
| Ehtimoliy yo'qotishlar hajmi bilan |
| Tahdid va risk bir xil tushunchalardir |
| Zarur investitsiyalar bilan |

**№ 196.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 2**

|  |
| --- |
| Xavf ma'lum bir manbaga tahdidni amalga oshirish mumkin bo'lgan zaiflik sifatida aniqlanganmi? |
| Ha |
| Yo'q |
| Ha, lekin hech qanday tahdid bo'lmasa |
| Agar tahdid bo'lsa, yo'q |

**№ 197.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Axborot xavfsizligi siyosatini ishlab chiqishda qanday asosiy qoidaga amal qilish zarur? |
| Muayyan aktivni himoya qilish qiymati aktivning o'z qiymatidan oshmasligi kerak |
| Axborot xavfsizligi siyosatini ishlab chiqish guruhi 20 kishidan oshmasligi kerak |
| Buzib kirish hujumlariga qanday javob berish kerak |
| Xavfsizlik tizimining ishlashi davomida qanday ma'lumotlarni yozib olish va kuzatish kerak |

**№ 198.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| CRAMM aniqlangan xavflar va ularning darajalariga mos keladigan qarshi choralari qatorida nechta umumiy tavsiyalar mavjud? |
| 300 ga yaqin |
| 1500 dan ortiq |
| 2000 dan ortiq |
| 10000 dan ortiq |

**№ 199.**

**Manba: 1-Ma‘ruza. Axborot xavfsizligi risklarini (xavf) boshqarish bo‘yicha asosiy tushunchalar, fanning maqsadi va vazifalari.**

**Qiyinlik darajasi – 3**

|  |
| --- |
| Axborot xavfsizligi sohasida risk deb nimaga aytiladi? |
| axborot tizimining xavfsizligini buzish natijasida yo'qotishlarning ehtimoliy miqdori |
| Tahdidning yuzaga kelishiga imkon beruvchi xususiyat |
| Qasddan yoki qasddan sodir bo'lishidan qat'i nazar, kompyuter tizimiga, shuningdek unda saqlanadigan va qayta ishlanadigan ma'lumotlarga nomaqbul ta'sir ko'rsatishi mumkin bo'lgan hodisa |
| Ma'lumotlarni uzatish tarmog'i orqali harakat qiluvchi buzg'unchi tomonidan yuzaga keladigan tahdidlar |

**№ 200.**

**Manba: 11- Ma‘ruza. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari**

**Qiyinlik darajasi – 2**

|  |
| --- |
| CRAMM zaiflik reytingi shkalasining qaysi qiymati o'rtacha har uch yilda bir marta sodir bo'ladigan insidentga mos keladi? |
| Past |
| o'rtacha |
| yuqori |
| juda baland |