

5330300 - Axborot xavfsizligi (sohalar bo'yicha) ta'lim yo'nalishi 4-bosqich talabalari uchun **“Axborot xavfsizligi xavflarni boshqarishga kirish”** fanidan **yakuniy nazorat savollari**

1. Risk, tahdid va zaiflik tushunchalariga ta'rif bering.
2. Axborot aktivi nima va u qanday obyektlarni o'z ichiga oladi?
3. Risklarni tahlil qilishning maqsadlarini tushuntirib bering.
4. Risklarni tahlil qilishning qanday bosqichlari bor?
5. “Galstuk-babochka” tahlili usuliga ta'rif bering.
6. “Galstuk-babochka” tahlilida ko'rsatilgan omillarini tushuntiring.
7. Rad etish daraxtining tahlili usuliga ta'rif bering.
8. Rad etish daraxtida ko'rsatilgan omillarini tushuntiring.
9. Vaziyatlar daraxtining tahlili usuliga ta'rif bering va u nima maqsadlarda qo'llaniladi.
10. Vaziyatlar daraxti qanday maqsadlarda qo'llaniladi hamda uning afzallik va kamchiliklari nimada?
11. Kontekstning qanday turlari mavjud?
12. Tashqi va ichki kontekstning farqlarini tushuntiring.
13. Kontekst dastlab riskni qaysi darajali baholashda o'rnatiladi?
14. Agar kontekst xavfni maqbul darajaga tushirish uchun zarur bo'lgan harakatlarni samarali aniqlash uchun yetarli ma'lumotni taqdim etsa, u holda risk ustida qanday harakatlar amalga oshiriladi?
15. Axborot aktivlarini identifikatsiya qilish jarayonini tushuntirib bering.
16. Birlamchi aktivning qiymatini identifikatsiya qilish.
17. Ikkilamchi aktivning qiymatini identifikatsiya qilish.
18. Axborot tizimlariga jismoniy kirish bilan bog'liq qanday tahdidlar mavjud?
19. AX risklarini baholash jarayoni qanday bosqichlarni o'z ichiga oladi?
20. AX risklarini baholash uchun an'anaviy yondashuvlarning asosiy metodologik kamchiliklari qanday? Ushbu kamchiliklarni bartaraf etish uchun qanday innovatsion yondashuvlardan foydalanish mumkin?
21. AX risklarini tahlil qilish jarayoni qanday bosqichlarni o'z ichiga oladi?
22. AX risklarini baholashning qaysi bosqichlarida biznes jarayonlari egalarining ishtiroki talab qilinishi mumkin va nima uchun?
23. Tashkilotning aktivlari ro'yxatini muntazam ravishda saqlab turish maqsadga muvofiqmi va bu AX risklarini baholash jarayoniga qanday ta'sir qilishi mumkin?
24. AXBTda AX risklarini baholash jarayonlari nimalardan iborat?
25. AX risklarini baholash jarayonining ishlashi natijasida tashkilot uchun eng muhim natijalar nima?
26. AX risklarini yuqori va batafsil tahlil qilish yondashuvlarining o'xshashligi va farqlari nimada?
27. Axborot xavfsizligi risklarini baholashning qanday usullari mavjud?
28. Axborot xavfsizligi risklarini sifat bo'yicha baholashning mohiyati

29. Axborot xavfsizligi risklarini miqdoriy baholash qanday amalga oshiriladi?
30. Risk darajasi va uning dolzarbligi nimani anglatadi?
31. Aniqlangan risklar bo'yicha qanday harakatlar amalga oshirilishi mumkin?
32. AX risklarini boshqarishning asosiy usullari qanday? Ularning har birining asosiy maqsadi nima?
33. Tashkilotda maqbul xavf darajasini hal qilish uchun kimlar yetarli vakolatlarga ega va nima uchun?
34. Qaysi ma'lumotlarga asoslanib, AX maqbul xavf darajasi haqida qaror qabul qilish kerak?
35. AX xavfini maqbul darajaga kamaytirish uchun qanday chora-tadbirlar mavjud?
36. AX risklarini qayta ishlash bo'yicha chora-tadbirlarni rejalashtirish qanday va kim tomonidan amalga oshiriladi?
37. AX risklarini saqlash va qabul qilish tushunchalarining farqi nimada?
38. AX risklarini saqlash va qabul qilish jarayonlarining kirish va chiqish ma'lumotlari qanday?
39. "AX risklariga munosabat" nima va u qanday amalga oshiriladi?
40. Axborot xavfsizligi risklariga munosabat faoliyatini amalga oshirishning maqsadlari qanday?
41. Axborot xavfsizligi xavflari qanday nazorat qilinadi va tekshiriladi?
42. Risk monitoringi nima va u qanday amalga oshiriladi?
43. AX risklarini monitoring qilish va qayta ko'rib chiqish qanday amalga oshiriladi?
44. AX xavf ko'rsatkichlarini monitoring qilish va qayta ko'rib chiqishning mohiyati nima?
45. Barcha AX risklarni boshqarish jarayonini monitoring qilish va qayta ko'rib chiqishning kirish va chiqish ma'lumotlari qaysilar?
46. CRAMM usulida avtomatlashtirilgan protseduralarni bajarish bosqichlari.
47. CRAMM usulining kuchli tomonlarini tavsiflang.
48. Potensial zararni baholash uchun CRAMM qanday parametrlardan foydalanishni tavsiya qiladi?
49. CRAMM aniqlangan xavflar va ularning darajalariga mos keladigan qarshi choralari qatorida nechta umumiy tavsiyalar mavjud?
50. CRAMM zaiflik reytingi shkalasining qaysi qiymati o'rtacha har uch yilda bir marta sodir bo'ladigan insidentga mos keladi?
51. Biznes uzluksizligi deganda nimalarni tushunasiz va u qanday amalga oshiriladi?
52. Uzluksiz ishni rejalashtirish asoslarini keltiring hamda ta'riflab bering.
53. Uzluksiz boshqarish rejasini sinash qanday amalga oshiriladi?
54. Biznesning muhim aktivlari qanday qiymatlarga ega?
55. Biznes uzluksizligini boshqarish kompleks boshqaruv jarayoni sifatida nimalarni o'z ichiga oladi?
56. Axborot xavfsizligi xavf-xatarlar tushunchasi nimanlarni o'z ichiga oladi?

57. “Axborot xavfsizligi xavf-xatarlarni boshqarish” atamasini qanday aniqlash mumkin?
58. Axborot xavfsizligi xavf-xatarlarini boshqarishning asosiy vazifalari nimalardan iborat?
59. Xatarlarni boshqarish jarayonining barcha asosiy komponentlarini sanab o‘ting va belgilang.
60. Axborot xavfsizligi xavf-xatarlarini boshqarish tizimi nima va uning qanday turlari mavjud.
61. Axborot xavfsizligi xavf-xatarlarini boshqarish jarayonining qaysi bosqichi eng ko‘p mehnat talab qiladi va nima uchun?
62. Axborot xavfsizligi xavf-xatarlarini boshqarish konteksti qanday aniqlanadi?
63. Axborot xavfsizligi xavf-xatarlarini baholashning mumkin bo‘lgan mezonlari qanday?
64. Axborot xavfsizligi xavflarining oqibatlarini (ta’sirini) baholash mezonlari qanday aniqlanadi?
65. Axborot xavfsizligi xavf-xatarlarini qabul qilishning mumkin bo‘lgan mezonlari qanday?
66. Axborot xavfsizligi xavf-xatarlarini boshqarish doirasi va chegaralari o‘rtasidagi farq nima?
67. Axborot xavfsizligi xavf-xatarlarini boshqarishda axborot xavfsizligi talablarini hisobga olish zarurati nimada? Ular qanday hisobga olinadi?
68. Risk menejmenti ma’lumotlari. Risk bo‘yicha axborot almashinuvi rejalari.
69. Qaror qabul qilishni rejalashtirish.
70. Riskni qayta ishlashda ustunliklarni o‘rnatish va qayta ishlash, qabul qilish bo‘yicha qarorlarni shakllantirish.
71. AXBT standartlarining turkumiga qanday standartlar kiradi?
72. AXBT standartlari turkumining vazifasi nimalardan iborat?
73. Tashkilot uchun AXBT standartlari turkumini qabul qilish natijasida amalga oshirilgan va barqaror muvaffaqiyatga erishish imkonini beradigan afzalliklar nimalarni o‘z ichiga oladi?
74. Axborot xavfsizligi risklarini boshqarish asosiy mezonlari, risklar ko‘lami va chegaralari.
75. Axborot xavfsizligi risklarini boshqarishda tashkilot tuzilmasi ahamiyati.
76. Ichki va tashqi kontekst. Risk mezonlari. Riskni baholash va qabul qilish
77. Qo‘llanish doirasi va chegaralarini aniqlashda tashkilotga tegishli qaysi ma’lumotlarni hisobga olish kerak?
78. Resurslarning qiymatini baholash mezonlari nimalardan iborat?
79. CRAMM usulining kamchiliklari.
80. CRAMM usuli doirasida avtomatlashtirilgan protseduralarni bajarish ketma-ketligi nimalardan iborat?
81. Tahdidan mumkin bo‘lgan yo‘qotishlarni taxmin qilish ketma-ketligi nimalardan iborat?

82. Tahdid qanday jismoniy zarar yetkazishi mumkin va bu qanday hisoblanadi?
83. Tahdid qancha mahsuldorlikni yo'qotishiga olib kelishi mumkin va bu qancha turadi?
84. Agar maxfiy ma'lumotlar oshkor qilinsa, kompaniya qanaqa zararlar ko'radi?
85. Tahdid ta'siridan qutulishning narxi qanday hisoblanadi?
86. Agar muhim qurilmalar ishlamay qolsa, yo'qotish qancha turadi?
87. Har bir aktiv va har bir tahdid uchun bitta hodisadan kutilgan zarar qancha (SLE – Single Loss Expectancy)?
88. Xavf monitoringi turlari qanday?
89. Risklarni boshqarish strategiyasini samarali monitoring va tahlil qilish usullari.
90. Aktivni sifat bo'yicha baholashda dastlabki xavfsizlik darajasi qanday aniqlanadi?
91. Tashkilotning axborot xavfsizligi xavfini baholashning umumlashtirilgan modeli.
92. Tahdidlarning dolzarbligini aniqlash usullari.
93. Dolzarbligi bo'yicha tahdidni baholash qoidalari.
94. Risk aniqlangandan keyingi riskni kamaytirish yo'llari.
95. "Galstuk-babochka" usulining afzallik va kamchiliklarini tushuntirib bering.
96. Rad etish daraxti usulining afzallik va kamchiliklarini tushuntirib bering.
97. Vaziyatlar daraxti usulining afzallik va kamchiliklarini tushuntirib bering.
98. Tashkilot axborot xavfsizligini ta'minlash tamoyillari.
99. Biznesning uzluksizligini ta'minlanishini boshqarishda axborot xavfsizligi masalalari.
100. Biznesning uzluksizligini ta'minlash bo'yicha rejalarni testdan o'tkazish, texnik xizmat ko'rsatish va qayta ko'rib chiqish.