60610300 - Axborot xavfsizligi 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 maqsadini tushuntirib bering.
4. Risklarni tahlil qilishning qanday bosqichlari bor?
5. “Galstuk-babochka” tahlili tushunchasiga ta’rif bering.
6. “Galstuk-babochka” tahlilida ko‘rsatilgan omillarini tushuntiring.
7. Rad etish daraxtining tahlili tushunchasiga ta’rif bering.
8. Rad etish daraxtida ko‘rsatilgan omillarini tushuntiring.
9. Vaziyatlar daraxtining tahlili tushunchasiga ta’rif bering.
10. Vaziyatlar daraxti qanday maqsadlarda qo‘llaniladi?
11. Kontekstning qanday turlari mavjud?
12. Tashqi va ichki kontekstning farqi nimada?
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 harakat amalga oshiriladi?
15. Axborot aktivlarini identifikatsiya qilish jarayonini tushintirib 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 va ularni bartaraf etish uchun innovatsion yondashuvlardan foydalanish.
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 jarayoni nima?
25. AX risklarini baholash jarayonining ishlashi natijasida tashkilot uchun eng muhim natijalar nima?
26. Telekommunkiatsiya tizimlaridagi xavflarni kamaytirish strategiyalari
27. Axborot xavfsizligi risklarini baholashning qanday usullari mavjud?
28. Axborot xavfsizligi risklarini sifat bo‘yicha baholashning mohiyati nimada?
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 yetarli vakolatlarga ega kim 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?
40. Tarmoq hujumlarida xavflarni kamaytirish strategiyalari.
41. Axborot xavfsizligi xavfi qanday nazorat qilinadi va tekshiriladi?
42. Risk monitoringi deb nimaga aytiladi?
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 usuli doirasida avtomatlashtirilgan protseduralarni bajarish bosqichlari.
47. CRAMM usulining kuchli tomonlarini tavsiflang.
48. Potentsial 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 nimani tushunasiz?
52. Uzluksiz ishni rejalashtirish asoslari.
53. Uzluksiz boshqarish rejasini sinash qanday amalga oshiriladi?
54. Biznesning boshqa muhim aktivlari kabi qiymatga ega bo‘lgan aktiv nima?
55. Biznes uzluksizligini boshqarish kompleks boshqaruv jarayoni sifatida nimani o‘z ichiga oladi?
56. Ilova sathida xavflarni kamaytirish strategiyalari.
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 komponentlari

60. Axborot xavfsizligi xavf-xatarlarini boshqarish tizimini belgilang.

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.

65. Axborot xavfsizligi xavf-xatarlarini qabul qilishning mumkin bo‘lgan mezonlari.

66. Axborot xavfsizligi xavf-xatarlarini boshqarish doirasi va chegaralari.

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. Hujum insidentlariga reaksiya bildirish o‘lchovlari.

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 mezoni. Riskni baholash, 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.

81. Tahdiddan mumkin bo'lgan yo‘qotishlarni taxmin qilish ketma-ketligi nimalardan iborat?

82. Tashkilotning uzluksiz ishlashini ta’minlash va boshqarish usullari.

83. Tahdid qancha mahsuldorlikni yo‘qotishiga olib kelishi mumkin va bu qancha turadi?

84. Aktivlarni identifikatsiya qilishdagi muxim chora-tadbirlar.

85. Riskni boshqarish sohasiga oid xalqaro va milliy standartlar.

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.

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.