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

1. Напишите определения следующих терминов (без объяснения): конфиденциальность, риск, актив.
2. Перечислите принципы управления рисками (УР).
3. Перечислите плюсы анализа «галстук-бабочка». Что такое внешний контекст. Объясните на примерах.
4. Напишите определения следующих терминов (без объяснения): целостность, угроза, средство управления/контроля.
5. Коротко объясните принцип УР: Интегрированный. (Integrated)
6. Перечислите плюсы анализа дерева неисправностей. Что такое внутренний контекст? Объясните на примерах.
7. Коротко объясните принцип УР: Структурированный и комплексный(всесторонний). (Structured and comprehensive)
8. Перечислите плюсы причинно-следственного анализа. Что такое установление контекста?
9. Коротко объясните принцип УР: Настроенный/индивидуальный. (Customized)
10. Перечислите минусы анализа «галстук-бабочка». Что такое критерий оценки. Объясните на примере.
11. Коротко объясните принцип УР: Инклюзивный. (Inclusive)
12. Перечислите минусы анализа дерева неисправностей. Что такое критерий воздействия. Объясните на примере.
13. Коротко объясните принцип УР: Лучшая доступная информация (Best available information).
14. Опишите порядок выполнения анализа «галстук-бабочка».Объясните, почему для управления рисками информационной безопасности важно знать стратегические цели организации.
15. Коротко объясните принцип УР: Человеческий и культурный факторы.
16. Опишите порядок выполнения анализа дерева неисправностей.
17. Объясните, почему для управления рисками информационной безопасности важно знать функции и структуру организации.
18. Напишите определения следующих терминов (без объяснения): доступность,событие , неопределенность (риск). Коротко объясните принцип УР: Непрерывное улучшение. (Continual improvement)
19. Опишите порядок выполнения причинно-следственного анализа.
20. Объясните, почему для управления рисками информационной безопасности важно учесть политику информационной безопасности организации.
21. Перечислите части процесса управления рисками информационной безопасности.
22. Объясните, почему для управления рисками информационной безопасности важно учитывать социокультурную среду, в которой находится организация.
23. Коротко объясните принцип УР: Интегрированный. (Integrated)

24. Что такое внутренний контекст? Объясните на примерах.
25. Коротко объясните принцип УР: Структурированный и комплексный(всесторонний). (Structured and comprehensive)
26. Критерий оценки актива.
27. Оценка вероятности инцидента. Измерение уровня риска
28. Зависимости и оценка влияния активов
29. Оценка риска
30. Идентификация риска.
31. Классификация рисков, составляющие риска.
32. Ценные активы организации. Оценка ценности актива.
33. Процесс менеджментом риска информационной безопасности
34. Анализ «дерева неисправностей». Приведите пример.
35. Что такое риск.
36. Внешний и внутренний контекст. Критерии оценивания риска.
37. Анализ «дерева событий». Приведите пример.
38. Цели управлению рисками ИБ.
39. Поддерживающие активы организации.
40. Причинно-следственный анализ. Приведите пример.
41. Критерии влияния и принятия риска ИБ.
42. Область применения и границы риска ИБ.
43. Основные (первичные) активы.
44. Проведите качественную и количественную оценку уровня исходной защищенности ценного актива. Нематериальные ресурсы(имидж организации).
45. Проведите качественную и количественную оценку уровня исходной защищенности ценного актива. Информационные ресурсы.
46. Оценка общего уровня исходной защищенности ценных активов организации.
47. Проведите качественную и количественную оценку уровня исходной защищенности ценного актива. Нематериальные ресурсы(кадры).
48. Оценка ущерба организации от нарушения информационной безопасности
49. Проведите качественную и количественную оценку уровня исходной защищенности ценного актива. Программное обеспечение.
50. Проведите качественную и количественную оценку уровня исходной защищенности ценного актива. Сетевые ресурсы.
51. Проведите качественную и количественную оценку уровня исходной защищенности ценного актива. WEB сайт.

52. Что включает в себя понятие риска ИБ?
53. Как можно определить термин «управление рисками ИБ»?
54. Каковы основные задачи управления рисками ИБ?
55. Перечислите и дайте определения всем основным составляющим процесса управления рисками.
56. Дайте определение системы управления рисками ИБ(СУРИБ).
57. Что входит в СУРИБ?

58. В каких режимах должна работать СУРИБ?
59. В чем суть применения системного подхода к СУРИБ?
60. Назовите этапы цикла PDCA применительно к СУРИБ.
61. Какой из этапов процесса управления рисками ИБ является наиболее трудоемким и почему?
62. Как определяется контекст управления рисками ИБ?
63. Каковы возможные критерии оценивания рисков ИБ?
64. Как определяются критерии оценки последствий (влияния) рисков ИБ?
65. Каковы возможные критерии принятия рисков ИБ?
66. В чем различие между областью действия и границами управления рисками ИБ?
67. В чем состоит необходимость учета требований по ОИБ при управлении рисками ИБ? Как они учитываются?
68. Какие этапы включает в себя процесс оценки рисков ИБ?
69. Каковы основные методологические недостатки традиционных подходов к оценке рисков ИБ? Применение каких инновационных подходов позволит устранить эти недостатки?
70. Какие этапы включает в себя процесс анализа рисков ИБ?
71. На каких этапах оценки рисков ИБ может потребоваться участие владельцев бизнес-процессов и почему?
72. Целесообразно ли вести реестр активов организации на регулярной основе и как это может повлиять на процесс оценки рисков ИБ?
73. Какое место процесс оценки рисков ИБ занимает в СУИБ?
74. Каковы наиболее значимые для организации результаты, получаемые в результате работы процесса оценки рисков ИБ?
75. На каком этапе цикла РБСЛ предполагает проведение первоначальной оценки рисков ИБ?
76. Что подразумевается под понятием актива? Какие типы активов учитываются при оценке рисков ИБ?
77. Что такое «угроза ИБ», «уязвимость», «источник угрозы ИБ»? Как взаимосвязаны эти понятия?
78. Каким образом возможно формировать каталоги угроз ИБ и уязвимостей, которые будут использоваться для оценки рисков ИБ?
79. В чем может состоять преимущество использования каталогов угроз ИБ, характерных для организации, в которой проводится оценка рисков ИБ, по сравнению с использованием типовых каталогов угроз ИБ?
80. Какие подходы к анализу рисков ИБ выделяются в стандартах?
81. В чем состоят сходства и различия подходов базового и детального анализа рисков ИБ?
82. Какой из подходов к анализу рисков ИБ предпочтительнее применять в небольшой организации, в которой эксплуатируются критичные системы, поддерживающие предоставление организацией услуг внешним заказчикам?
83. В какой ситуации и для какой организации целесообразно применять комбинированный подход к анализу рисков ИБ?
84. Какие подходы к оценке рисков ИБ выделяются в стандартах?

85. Как осуществляются качественная, количественная и гибридная оценка рисков ИБ?
86. В чем суть процесса оценивания рисков ИБ?
87. Какие основные способы обработки рисков ИБ? В чем основная цель каждого из них?
88. Кто в организации обладает достаточными полномочиями для принятия решения об уровне приемлемого риска ИБ и почему?
89. На основе какой информации должно приниматься решение об уровне приемлемого риска ИБ?
90. Какие существуют меры по снижению рисков ИБ до приемлемого уровня?
91. Каким образом и кем осуществляется планирование мер по обработке рисков ИБ?
92. В чем отличие понятий сохранения и принятия рисков ИБ? Каковы входные и выходные данные этих процессов?
93. Что такое «коммуникация рисков ИБ»? Каковы цели осуществления деятельности по коммуникации рисков ИБ?
94. Основные различия между высокоуровневой и детальной оценкой риска
95. Как осуществляется мониторинг и пересмотр рисков ИБ?
96. В чем заключается суть мониторинга и пересмотра показателей рисков ИБ?
97. Каковы входные и выходные данные мониторинга и пересмотра всего процесса управления рисками ИБ?
98. Что входит в документальное обеспечение управления рисками ИБ?
99. Охарактеризуйте документ «Политика управления рисками ИБ».
100. Методология CRAMM (CCTA Risk Analysis and Management Method)
101. Стратегии снижения рисков атак на уровне приложений и представлений
102. Типичные атаки на уровне приложений и представлений, стратегии снижения рисков.
103. Структура CRAMM
104. Назовите документы процесса управления рисками ИБ операционного уровня.
105. Что отражается в плане обработки рисков ИБ?
106. На каких этапах оценки рисков ИБ использование инструментальных средств управления рисками ИБ может принести наибольшую пользу?
107. Особенности рисков телекоммуникационных и сетевых атак
108. Ключевые стратегии снижения рисков телекоммуникационных и сетевых атак
109. Современные технологии защиты телекоммуникационных и сетевых атак.
110. Какие критерии необходимо учитывать при выборе инструментальных средства управления рисками ИБ?