**Примерные оценочные материалы, применяемые при проведении**

**промежуточной аттестации по дисциплине «Стандартизация и сертификация систем информационной безопасности»**

При проведении промежуточной аттестации обучающемуся предлагается дать ответы на 3 вопроса из нижеприведенного списка.

1. Техническое регулирование, стандартизация и сертификация. Определения и понятия.
2. Стандартизация и ее основные принципы.
3. Техническое регулирование и его принципы.
4. Международный и национальный стандарты.
5. Унификация и агрегатирование: содержание и применение.
6. Симплификация и типизация: содержание и применение.
7. Нормативные документы по стандартизации.
8. Виды национальных стандартов.
9. Федеральное агентство по техническому регулированию и его функции.
10. Сертификация и ее основные этапы.
11. Добровольная и обязательная сертификация.
12. Функции органа по сертификации.
13. Схемы декларирования соответствия.
14. Обязанности органа по сертификации.
15. Система сертификации систем качества и производств (регистр систем качества).
16. Органы и службы стандартизации РФ.
17. Центры стандартизации и метрологии (ЦСМ) и их функции.
18. Виды национальных стандартов РФ.
19. Общероссийские клас­сификаторы технико-экономической информации (ОКТЭИ).
20. Комплексная и опережающая стандартизации.
21. Межотраслевые системы стандартов.
22. Параметрическая стандартизация.
23. Основные принципы организации сертификации в РФ.
24. Сертификация в Законе «О техническом регулировании».
25. Технические регламенты Таможенного союза и Евразийского экономического союза.
26. Виды сертификации продукции.
27. Формы сертификации продукции.
28. Продукция, подлежащая обязательной сертификации.
29. Органы, выдающие сертификаты.
30. Проверка подлинности сертификата.
31. Ответственность за подделку сертификата.
32. Сертификация производства в РФ.
33. Организации – разработчики стандартов вычислительных систем и сетей: ISO, ITU, IEEE, ECMA, CBEMA, EIA, ANSI.
34. Стандартизация сетей.
35. Стандартизация в телекоммуникациях.
36. Стандартизация компьютерных систем.
37. Понятия интерфейса, протокола и стека.
38. Модель OSI: 7 уровней протоколов сети.
39. Методы коммутации в компьютерных сетях.
40. ГОСТы на автоматизированные системы: ГОСТ Р 59793–2021, ГОСТ 34.602–2020.
41. ГОСТы для высокопроизводительных вычислительных систем: ГОСТ Р 57700.36-2021, ГОСТР 57700.27— 2020.
42. Жизненный цикл ПО и его стандартизация.
43. Модели разработки ПО: каскадная, спиральная.
44. Стандартизация спецификаций программных модулей.
45. Стандартизация проектирования и кодирования ПО.
46. Оценка качества ПО в ГОСТах: ГОСТ 28195 и ИСО/МЭК 9126.
47. Системная и программная инженерия в ГОСТах: ГОСТ 25001-2017, ГОСТ 25051-2017, ГОСТ 25010-2015.
48. Проблема стандартизации в области информационной безопасности в международных и национальных стандартах.
49. ГОСТы серии 27000.
50. Стандартизация терминологии в ISO/IEC 27000.
51. Стандартизация базовых требований в ISO/IEC 27001/27002.
52. Стандартизация порядка внедрения СМИБ в ISO/IEC 27003.
53. Стандартизация основных процессов в ISO/IEC 27004/27005/27007.
54. Стандартизация корпоративного управления СМИБ в ISO/IEC 27014/27016.
55. Стандартизация кибербезопасности в ISO/IEC 27103.
56. Система ГОСТов в области защиты информации: ГОСТ Р 52069.0-2013.
57. Общие технические требования к защите от несанкционированного доступа к информации в ГОСТ Р 50739.
58. Основные требования и определения в ГОСТ Р 50922.
59. Порядок создания автоматизированных систем в защищенном исполнении в ГОСТ Р 51583.
60. Стандартизация номенклатуры качества защиты информации в ГОСТ Р 52447.
61. Стандартизация требований к средствам высоконадежной биометрической аутентификации в ГОСТ Р 52633.
62. Международный стандарт ISO/IEC TR 19759-2015 (SWEBOK  (Software Engineering Body of Knowledge).
63. Ядро знаний SWEBOK и международный стандарт  ISO/IEC 12207:2008 Systems and software engineering — Software life cycle processes.
64. Процессы жизненного цикла программного обеспечения (ISO/IEC 12207:2008).
65. Основные процессы жизненного цикла ПО.
66. Вспомогательные процессы жизненного цикла ПО.
67. Организационные процессы жизненного цикла ПО.
68. Основные области знаний SWEBOK.
69. Области управления SWEBOK.
70. Инженерия требований к ПО.
71. Национальная Программа "Цифровая экономика Российской Федерации" и ее Федеральные проекты.
72. Федеральный проект «Цифровое государственное управление» и проблема стандартизации и унификации представления правовой информации.
73. Федеральный проект «Информационная безопасность» и проблема стандартизированных, сертифицированных по требованиям информационной безопасности решений для типовых объектов КИИ.
74. Федеральный проект «Кадры для цифровой экономики» и проблема стандартизации оценки профессиональных компетенций для использования в онлайн сервисах для проведения трудоспособными гражданами самооценки своих компетенций
75. Федеральный проект «Информационная инфраструктура» и проблема стандартизации классификации ЦОД.
76. Федеральный проект «Искусственный интеллект» и проблемы стандартизации и сертификации.
77. Стандартизация и унификация представления правовой информации для цифровой платформы «Государственная система правовой информации».
78. ПНСТ «Умное производство. Двойники цифровые производства» (части 1-4).
79. ПНСТ «Информационные технологии. Умный город. Функциональная совместимость».
80. ПНСТ «Информационные технологии. Умный город. Руководства по обмену и совместному использованию данных».
81. ПНСТ «Информационные технологии. Интернет вещей. Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением».
82. Федеральная служба по техническому и экспортному контролю (ФСТЭК), ее цели, задачи
83. Нормативные документы ФСТЭК в области информационной безопасности вычислительных комплексов, систем и сетей.
84. Приказ ФСТЭК №17 от 11.02.2013. Меры защиты информации в государственных информационных системах.
85. Методика ФСТЭК для оценки угроз безопасности. Базовая модель угроз безопасности персональных данных при обработке в ИС.
86. Специальные требования и рекомендации ФСТЭК по технической защите конфиденциальной информации (СТР-К).