Приложение к рабочей программе дисциплины (практики)

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН)

Факультет искусственного интеллекта

(наименование основного учебного подразделения)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

Освоение дисциплины (практики) ведется в рамках реализации основной профессиональной образовательной программы (ОП ВО, профиль/ специализация):

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(направленность (профиль) ОП ВО)

Москва, 2025

1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций, формируемых в процессе освоения дисциплины содержится в Разделе 2. «Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине».

Примеры практико-ориентированных (ситуационных) заданий

Задача 1. Составьте модель угроз нарушения информационной безопасности для автоматизированной системы коммерческой организации.

Задача 2. Составьте проект классификатора инцидентов ИБ.

Задача 3. Переформулируйте требования стандарта PCI DSS в терминах стандарта ГОСТ Р 57580.1.

Задача 4. В ходе проведенной службой информационной безопасности банка проверки были выявлены учетные записи ранее уволенных сотрудников. Предложите способы недопущения таких событий при следующих проверках со стороны службы ИБ.

Задача 5. В корпоративной сети кредитной организации выявлено автоматизированное рабочее место, на котором не установлен антивирус. Опишите возможные риски информационной безопасности, которые могут возникнуть.

Задача 6. Составьте развернутый план частной политики менеджмента инцидентов ИБ.

Примерный перечень вопросов для подготовки к зачету

1. Системный подход к исследованию объектов информационной безопасности. Особенности рассмотрения системного подхода применительно к управлению.
2. Какие виды деятельности в организации можно назвать процессом (или бизнес-процессом)?
3. Что понимается под ресурсами и управляющим воздействием в рамках определения понятия процесса?
4. Система управления информационной безопасности, основанная на процессном подходе.
5. К каким процессам организации может быть применена циклическая модель PDCA?

6. Основные преимущества использования ситуационного подхода в системе управления информационной безопасности?

7. Раскрыть принципы процессного подхода.

8. Классы информационных ресурсов

9. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

10. Для организаций какой сферы применимы стандарты серии ISO/IEC 27000?

11. Каковы отличительные черты стандартов серии ISO/IEC 27000?

12. Какой из стандартов серии ISO/IEC 27000 содержит требования к созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

13. На основании чего может проводиться оценка эффективности СУИБ?

14. Можно ли проводить аудит (или сертификацию) на соответствие стандарту ISO/IEC 27002 (бывший ISO/IEC 17799)?

15. Каковы основные идеи руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ?

16. Почему подход к проведению аудита систем менеджмента качества и окружающей среды, изложенный в стандарте 1SO/IEC 19011, может быть применен для проведения внутренних аудитов СУИБ?

17. В каком стандарте серии ISO/IEC 27000 описана инфраструктура руководства ИБ?

18. В чем состоят преимущества использования (учета) требований российских и международных стандартов по управлению ИБ при построении СУИБ или отдельных процессов управления ИБ?

19. Каковы преимущества одновременного учета требований стандартов, предъявляемых как к СУИБ в целом, так и к отдельным процессам, разрабатываемым в рамках СУИБ?

20. В чем может заключаться различие между требованиями к системам управления непрерывностью бизнеса и к процессу управления непрерывностью бизнеса?

21. Какие тенденции характерны для развития стандартизации управления ИБ в Российской Федерации?

22. Каково значение стандартов серии СТО БР ИББС в рамках развития стандартизации управления ИБ в России?

23. Какие аспекты регламентируют стандарты серии СТО БР ИББС, если говорить об управлении ИБ?

24. Каковы цели и задачи стандартизации по ОИБ организаций БС РФ?

25. Каковы основные цели проведения аудита ИБ организаций БС РФ?

26. На основе какой методики рекомендуется проводить оценку соответствия уровня ИБ организации БС РФ требованиям стандарта СТО БР ИББС-1.0?

27. Понятия политики обеспечения ИБ и политики ИБ организации

28. Сущность и содержание политики информационной безопасности организации.

29. Иерархия документов в области ОИБ для организации БС РФ.

30. Практика при выборе области действия СУИБ. Какие стратегии выбора области действия СУИБ существуют? Какие факторы необходимо учитывать при выборе области действия СУИБ?

31. Что входит в документальное обеспечение СУИБ? Каковы этапы его жизненного цикла СУИБ.

32. Дайте определения ОИБ, управления ИБ и СУИБ организации.

33. Опишите деятельность по ОИБ организации как процесс. Каковы его входные и выходные данные, ресурсы и управляющие воздействия?

34. Как процесс ОИБ в организации связан с процессами ее основной деятельности?

35. Каковы основные этапы процесса управления ИБ ИТТ?

36. Что является хорошей практикой при выборе области действия СУИБ? Какие стратегии выбора области действия СУИБ существуют?

37. Какие факторы необходимо учитывать при выборе области действия СУИБ?

38. Какие параметры процессов являются наиболее значимыми при выборе области действия проектируемой СУИБ?

39. Что входит в документальное обеспечение СУИБ? Каковы этапы его жизненного цикла?

40. Какие уровни документов включает в себя иерархия документов СУИБ? Какие виды конкретных документов создаются на каждом из уровней?

41. Какова взаимосвязь между понятиями «Политика ИБ» и «Политика СУИБ»?

42. Что должна включать в себя политика СУИБ?

43. На каких этапах руководство организации должно продемонстрировать свою приверженность к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

44. В чем состоит основная необходимость участия высшего руководства в жизненном цикле СУИБ?

45. Какие действия и процессы выполняются на стадии совершенствования СУИБ, задачи данного этапа?

46. В чем разница и сходство между понятиями корректирующего и предупреждающего действий?

47. Почему в рамках процессного подхода к управлению ИБ следует особое внимание уделять мониторингу и анализу результативности и эффективности СУИБ?

48. В чем состоят различия между такими основными свойствами процессов, как эффективность и результативность?

49. Какие этапы включает в себя идентификация процессов управления ИБ в организации и какие действия необходимо предпринять в рамках этих этапов?

50. Какие действия и процессы выполняются на стадии планирования СУИБ? Каковы задачи данного этапа?

51. Специалистов каких подразделений необходимо включать в рабочую группу по построению СУИБ и почему?

52. Какие действия и процессы выполняются на стадии реализации и внедрения СУИБ, задачи данного этапа?

53. Какие действия и процессы выполняются на стадии проверки СУИБ, задачи данного этапа?

54. Какие действия и процессы выполняются на стадии совершенствования СУИБ, задачи данного этапа?

55. Разработка, проектирование СУИБ как единый процесс. Реализация процесса СУИБ. Контроль СУИБ процесса в целом. Совершенствование процесса СУИБ

56. Описание объекта. Описание основных бизнес-процессов.

57. Идентификация активов. Описание активов

58. Оценка рисков ИБ. Перечень актуальных угроз

59. Документы административного уровня. Требования, содержание и примеры документов этого уровня.

60. Документы второго уровня (верхнего). Требования, содержание и примеры документов этого уровня.

61. Документы технического уровня. Требования, содержание и примеры документов этого уровня.

62. Документы нижнего уровня. Требования, содержание и примеры документов этого уровня.

63. Понятие аудита информационной безопасности. Государственные стандарты Российской Федерации в сфере аудита информационной безопасности

64. Нормативная база аудита информационной безопасности

65. Эксплуатация и независимый аудит СУИБ

66. Лицензирование и сертификация деятельности в области защиты информации

67. Методика проведения аудита информационной безопасности

68. Определение, оповещение и регистрация инцидентов ИБ.

69. Расследование или анализ инцидентов, с целью предотвращения повторного их проявления.

70. Основные задачи процесса реагирования на инциденты ИБ и применение превентивных мер защиты для устранения причин потенциального ущерба

71. Основные процессы СУИБ. Обязательная документация СУИБ

72. Эксплуатация и независимый аудит СУИБ

73. Внедрение разработанных процессов. Документ «Положение о применимости»

74. Раскройте цель и задачи процесса «Обеспечение непрерывности ведения бизнеса»

75. Раскройте цель и задачи процесса «Управление инцидентами ИБ».

Примерный перечень теоретических вопросов для подготовки к экзамену

1. Какие действия и процессы составляют стадию проверки СУИБ?

2. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии разработки технических заданий?

3. Что такое информационная безопасность, информационная безопасность объекта информатизации, безопасность информации, безопасность информационной технологии, киберустойчивость (в финансовой сфере)?

4. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии проектирования?

5. Что такое система менеджмента организации и система менеджмента информационной безопасности организации?

6. В чем заключается процессный подход к управлению ИБ?

7. Какие действия и процессы составляют стадию планирования СУИБ?

8. Что такое угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ?

9. Что такое циклическая модель PDCA применительно к управлению ИБ?

10. Что включает выбор и применение финансовой организацией мер ЗИ согласно ГОСТ Р 57580.1-2017?

11. В каких случаях, согласно ГОСТ Р 57580.1-2017, возможно использование компенсирующих мер ЗИ? Какие условия при этом должны быть выполнены?

12. Что такое контур безопасности и уровень защиты информации, согласно ГОСТ Р

57580.1-2017? Кем и на основании чего устанавливается уровень ЗИ финансовой организации для конкретного контура безопасности?

13. Укажите стадии жизненного цикла автоматизированных систем. Чем обусловлены особенности обеспечения информационной безопасности автоматизированных систем на различных стадиях жизненного цикла?

14. Назовите основные нормативно правовые документы в области управления информационной безопасности.