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)

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

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

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(направленность (профиль) ОП ВО)

Москва, 2025

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

1. Паспорт фонда оценочных средств

Направление подготовки: 10.03.01 «Информационная безопасность» (программа подготовки бакалавра).

№ п/п	Контролируемые разделы (темы) дисциплины	Наименование оценочного средства
1	Выявление уязвимых элементов, через которые возможна реализация угроз информационной безопасности предприятия	Письменный экспресс-опрос на семинаре с выставлением оценок в балльной системе
2	Принципы организации КСЗИ на предприятии и этапы разработки	Письменный экспресс-опрос на семинаре с выставлением оценок в балльной системе
3	Технологическое, организационное, кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ на предприятии.	Письменный экспресс-опрос на семинаре с выставлением оценок в балльной системе
4	Каналы несанкционированного доступа к информации предприятия через Интернет.	Письменный экспресс-опрос на семинаре с выставлением оценок в балльной системе
5	Модели оценки угроз информационной безопасности и оценка эффективности функционирования КСЗИ на предприятии.	Письменный экспресс-опрос на семинаре с выставлением оценок в балльной системе
6	Создание политик безопасности	Письменный экспресс-опрос на семинаре с выставлением оценок в балльной системе.

2. Виды контроля по периодам обучения

2.1 Материалы для проведения текущего контроля.

2.1.1. Форма текущего контроля – письменный экспресс-опрос на семинаре с выставлением оценок в балльной системе.

2.1.2. Перечень вопросов (заданий).

Задание № 1. Выявление направленности угроз информационной безопасности предприятия.

Вопрос №1. Информационная безопасность: сущность и содержание. Защита информации в обеспечении информационной безопасности и ее задачи.

Вопрос № 2. Организационные основы обеспечения информационной безопасности. Требования международных стандартов по вопросам организации обеспечения информационной безопасности.

Вопросы для самоконтроля:

1. Объекты, методы и система обеспечения информационной безопасности.
2. Понятие об информационном объекте и его элементах.
3. Условия и факторы, оказывающие влияние на организационную структуру системы обеспечения информационной безопасности.
4. Принципы организационного обеспечения информационной безопасности.
5. Силы и средства обеспечения информационной безопасности.

Проблемные вопросы:

1. Нейтрализация угроз информационной безопасности социотехнического оюъекта.
2. Соответствие требованиям международных стандартов по вопросам организации обеспечения информационной безопасности и уровень информационной безопасности предприятия.

Задание № 2. Принципы организации КСЗИ на предприятии и этапы разработки КСЗИ.

Вопрос № 1. Принципы организации КСЗИ. Классификация АСУ по защищенности от несанкционированного доступа.

Вопрос № 2. Разработка проекта КСЗИ.

Вопросы для самоконтроля:

1. Требования к защищенности АСУ.

2. Аттестация систем защиты и обучение пользователей.

Проблемные вопросы:

1. Задачи администрации по внедрению системы обеспечения информационной безопасности и защиты информации.

2. Внедрение комплексной системы защиты информации на предприятии.

Задание № 3. Обеспечение функционирования КСЗИ на предприятии.

Вопрос № 1. Технологическое обеспечение и процессный подход к обеспечению информационной безопасности. Стандарты, базирующиеся на процессном подходе к обеспечению информационной безопасности.

Вопрос № 2. Принципы организационного обеспечения информационной безопасности и структура системы обеспечения.

Вопрос № 3. Направления и методы работы с персоналом в интересах защиты информации.

Вопрос № 4. Правовые нормы в обеспечении информационной безопасности. Право и его роль в регулировании комплекса отношений в информационной сфере. Отрасли права, обеспечивающие законность в интересах информационной безопасности.

Вопрос № 5. Инвентаризация информационных ресурсов компании.

Вопросы для самоконтроля:

1. Модель Деминга-Шухарта как основа организации процесса обеспечения информационной безопасности.

2. Силы и средства обеспечения информационной безопасности предприятия.

3. Роль подразделения защиты информации в системе обеспечения информационной безопасности.

4. Проверочные мероприятия, обучение работе с конфиденциальной информацией и оформление допуска к ней при приеме на работу.

5. Структура и направленность правовых мер обеспечения информационной безопасности.

6. Сертифицированные программно-аппаратные средства защиты информации.

Проблемные вопросы:

1. Технологии обеспечения информационной безопасности и роли в системе ее обеспечения руководства предприятием.

2. Мониторинг осведомленности персонала о тайнах работодателя.

Задание № 4. Каналы несанкционированного доступа к информации предприятия через Интернет.

Вопрос № 1. Угрозы безопасности, связанные с подключением компании к сети Интернет.

Вопрос № 2. Обеспечение защищённого подключения к Интернет на основе сервера терминальных служб.

Вопрос № 3. Создание защищённой системы электронного документооборота на основе технологии инфраструктуры открытого ключа.

Вопросы для самоконтроля:

1. Внешние угрозы интернет-порталу.

2. Подсистемы КСЗИ: разграничения доступа к ресурсам портала, обнаружения и предотвращения сетевых атак, контроля целостности, межсетевого экранирования.

3. Методы организации защищённого подключения к Интернету на основе наложенных средств защиты.

4. Использование USB-ключей eToken в качестве хранилища цифровых сертификатов и секретных ключей пользователей.

Проблемные вопросы:

1. Проведение аудита интернет-узлов предприятия.

2. Соответствие удостоверяющего центра требованиям международных стандартов.

Задание № 5. Модели оценки угроз информационной безопасности и оценка эффективности функционирования КСЗИ на предприятии.

Вопрос № 1. Сущность и модели вирусных угроз и спама.

Вопрос № 2. Содержание понятия «риски» и технологии их анализа в интересах защиты информации. Особенности применения инструментальных средств оценки рисков на примере программного комплекса MSAT (Microsoft Security Assessment Tool).

Вопрос № 3. Сущность и содержание аудита информационной безопасности. Инструментальные средства анализа информационной безопасности.

Вопросы для самоконтроля:

1. Уязвимости информационных объектов в связи с атаками из сети Интернет.

2. Понятие качественной и количественной оценки рисков, шкалы и критерии измерения.

3. Комплексная оценка рисков безопасности и ее основные этапы.

4. Критерии оценки уровня информационной безопасности предприятия.

5. Методика оценки рисков OCTAVE.

6. Требования COBIT в реализации аудита информационной безопасности.

Проблемные вопросы:

1. Оценка текущего состояния информационной безопасности компании.

2. Соответствие системы управления информационной безопасностью предприятия требованиям стандарта ISO 27001.

Задание № 6. Создание политик безопасности.

Вопрос № 1. Содержание политики безопасности информационно-телекоммуникационных технологий.

Вопрос № 2. Инциденты и эскалации в практике КЗИ.

Вопросы для самоконтроля:

1. Особенности выработки официальной политики предприятия в области информационной безопасности и управления безопасностью.

2. Эскалации в практике защиты информации

Проблемный вопрос.

1. Инциденты и реагирование на них в текущей работе предприятия.

Материалы для проведения промежуточной аттестации:

Вид промежуточной аттестации – экзамен.

Форма проведения – устный опрос.

Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию.

1. Функции и задачи защиты информации.

2. Классы задач защиты информации.

3. Требования к информации, принципы организации КСЗИ и критические факторы успеха защиты информации.

4. Сущность и структура системы обеспечения информационной безопасности и требования к системе защиты информации.

5. Организационное построение КСЗИ, структура и содержание цикла работ по защите информации.

6. Управление защитой информации, повышение эффективности защиты и реализация технологий, обеспечивающих информационную безопасность предприятия.

7. Роль органов управления предприятием в выполнении задач защиты информации.

8. Принципы построения, задачи создания и содержание базовых программ системы подготовки и переподготовки персонала по вопросам защиты информации.

9. Принципы организационного обеспечения и структура системы обеспечения информационной безопасности.

10. Силы обеспечения информационной безопасности предприятия и задачи службы информационной безопасности.

11. Средства обеспечения информационной безопасности предприятия.

12. Информационно-правовые нормы и их классификация.

13. Технико-правовые нормы, их значение, функции и классификация.

14. Направленность правовых мер обеспечения информационной безопасности.

15. Сущность и средства технического обеспечения информационной безопасности.

16. Цели материального обеспечения и направления функционирования его органов.

17. Информационные и сетевые ресурсы и методики их инвентаризации.

18. Система сертификации и сертифицированные программно-аппаратные средства защиты информации.

19. Требования к выбору средств защиты информации и рекомендации по их использованию.

20. Сущность, цель и основные задачи технологического обеспечения информационной безопасности.

21. Сущность, функции управления и общая структура системы управления как технологической основы построения КСЗИ.

22. Сущность, принципы и модели процессного подхода в обеспечении информационной безопасности

23. Применение нотаций IDEF в описании технологических процессов совершенствования информационной безопасности

24. Оптимизация, реинжиниринг и автоматизация как методы совершенствования информационной безопасности.

25. Система менеджмента качества как метод совершенствования информационной безопасности.

26. Сущность и содержание процессного подхода в управлении информационной безопасностью. Модель Деминга-Шухарта как основа современной организации процесса обеспечения информационной безопасности.

27. Содержание алгоритма внедрения системы менеджмента информационной безопасности, предусмотренного Международным стандартом ISO 27001.

28. Функции, направления и методы работы с персоналом в интересах обеспечения информационной безопасности.

29. Методы анализа информационного объекта.

30. Особенности приема сотрудников на работу, связанную с конфиденциальной информацией.

31. Процедуры приема сотрудников, работа которых связана с конфиденциальной информацией.

32. Проверочные мероприятия в ходе приема на работу, связанную с конфиденциальной информацией.

33. Принципы построения и особенности функционирования разрешительной системы предприятия.

34. Мониторинг осведомленности персонала о тайнах работодателя.

35. ГОСТ Р ИСО/МЭК 13335-3-2006 о сущности, роли, месте политики информационной безопасности и взаимосвязи с политиками безопасности предприятия

36. Структура и базовые принципы политики информационной безопасности.

37. Исходные данные для формирования политики
информационной безопасности и уровни документирования ее требований.

38. Основное содержание документа «Политика информационной безопасности предприятия» соглас-но требованиям ГОСТ Р ИСО/МЭК 13335-3-2006.

39. ГОСТ Р ИСО/МЭК 13335-3-2006 о целях, стратегии и элементах политики безопасности информационных технологий.

40. ГОСТ Р ИСО/МЭК 13335-3-2006 о перечне вопросов политики ИТТ-безопасности.

41. ГОСТ Р ИСО/МЭК 13335-3-2006 о подходах к выработке политики безопасности информационных технологий.

42. ITIL service support-модель о подходах к управлению обслуживанием и содержании управления проблемами.

43. Содержание обеспечения сервисов и управления инцидентами.

44. Содержание обеспечения сервисов и управления качеством.

45. Принципы эффективной политики реагирования на инциденты информационной безопасности.

46. Сущность отказа в обслуживании, сбора информации и несанкционированного доступа как инцидентов информационной безопасности.

47. ГОСТ Р ИСО/МЭК ТО 18044-2007 о политике менеджмента и расследования инцидентов информационной безопасности.

48. Модели команды, ресурсы и инструментарий расследования инцидентов информационной безопасности.

49. Сущность, задачи, организационные роли уровней управления инцидентами и распределение ответственности между ними.

50. Сущность и содержание процессов управления инцидентами, контроля проблем и контроля ошибок согласно ITIL service support-модели.

51. Содержание и виды эскалаций в управлении инцидентами согласно ITIL service support-модели.

52. Содержание понятия «риски» в защите информации и алгоритм их анализа в интересах комплексной защиты информации.

53. Идентификация рисков применительно к каталогам угроз в стандарте IT Baseline Protection Manual и алгоритм их анализа.

54. Понятие качественной и количественной оценки рисков, шкалы и критерии измерения.

55. Комплексная оценка рисков безопасности, ее основные этапы и особенности применения инструментальных средств оценки рисков на примере программного комплекса Microsoft Security Assessment Tool (MSAT).

56. Критерии оценки уровня информационной безопасности предприятия. Методика оценки рисков OCTAVE.

57. Подходы к оценке угроз безопасности КСЗИ по материалам «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК от 15 февраля 2008 г.

58. Угрозы безопасности, связанные с подключением компании к сети Интернет.

59. Подсистемы КСЗИ, связанные с подключением компании к сети Интернет: разграничения доступа к ресурсам портала, обнаружения и предотвращения сетевых атак, контроля целостности, межсетевого экранирования.

60. Обеспечение защищённого подключения к Интернет на основе сервера терминальных служб и методов на основе наложенных средств защиты.

61. Аудит Интернет-узлов компаний (Penetration Testing), направленный на оценку соответствия системы управления информационной безопасностью требованиям стандарта ISO 27001.

62. Сущность, цель и задачи аудита информационной безопасности. Модель зрелости процессов менеджмента информационной безопасности и параметры достижения уровней зрелости (на примере БС РФ).

63. Перечень исходных данных для аудита информационной безопасности. Информация, подлежащая сбору и анализу для проведения аудита.

64. Направления, стадии, методы и методики обследования в ходе аудита.

65. Состав работ по проведению аудита и структура аудиторского отчета.

66. Требования COBIT по реализации аудита информационной безопасности.

67. Инструментальные средства анализа информационной безопасности. Требования безопасности Microsoft Security Assessment Tool (MSAT).

68. Системы COBRA и КОНДОР как программные продукты для проверки рисков базового уровня требований стандарта ISO 17799.

69. Создание защищённой системы электронного документооборота на основе технологии инфраструктуры открытого ключа.

70. Удостоверяющий центр как основа для управления цифровыми сертификатами пользователя.

71. Алгоритмы оценки информационной обстановки в интересах управления информационной безопасностью.

72. Сущность и цели аналитической деятельности в обеспечении информационной безопасности. Определения понятий: «цель», «задача», «проблема», «решение», «метод», «способ», «анализ», «аналитика».

73. Аналитическая технология и типовые аналитические задачи обеспечения информационной безопасности.

74. Сущность и содержание системного анализа информационной сферы.

Критерии и показатели оценки.

Оценивание знаний студентов осуществляется в ходе текущего контроля успеваемости и промежуточной аттестации в соответствии с балльно-рейтинговой системой ФИБ.

Оценка знаний студентов включает:

1. Оценку работы студента в течение семестра – до 60 баллов.
2. Оценка знаний студента на зачете – до 40 баллов.

3.1 Порядок выставления общей оценки в рамках дифференцированного зачета (экзамена).

Для получения 35-40 баллов за ответ на один вопрос зачета студент должен:

1. Исчерпывающе владеть терминологическим аппаратом по теме, ее метаязыком; видеть системные связи объекта с общим контекстом дисциплины и смежными вопросами.

2. Иметь системное представление об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Владеть методикой анализа объекта, видеть связь теоретических аспектов темы с прикладными исследованиями.

4. Уметь выстраивать связные научные формулировки ответа с опорой на базовые понятия и категории; проявлять необходимую степень самостоятельности в представлении темы в ее внутренней логике.

Для получения 25-34 баллов за ответ на один вопрос зачета студент должен:

1. В достаточной мере владеть терминологическим аппаратом по теме; видеть системные связи объекта со смежными вопросами.

2. Иметь общее представление об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Владеть основными принципами методики анализа объекта, видеть связь теоретических аспектов темы с прикладными исследованиями.

4. Уметь выстраивать связные научные формулировки с опорой на базовые понятия и категории; проявлять необходимую степень самостоятельности в представлении темы в ее внутренней логике.

Для получения 15-24 баллов за ответ на один вопрос зачета студент должен:

1. В достаточной мере владеть терминологическим аппаратом по теме, не допуская серьезных ошибок понятийного характера.

2. Иметь минимально необходимое представление об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Владеть основными принципами методики анализа объекта, не допуская серьезных ошибок при характеристике объекта.

4. Уметь выстраивать научные формулировки с опорой на базовые понятия и категории.

Менее 15 баллов за ответ на один вопрос зачета выставляется студенту в том случае, если он:

1. Не владеет терминологическим аппаратом по теме.

2. Не имеет представлений об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Не владеет принципами анализа объекта.

4. Не умеет выстраивать связные научные формулировки.

2.