МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

Кафедра «Информатика и вычислительная техника»

УТВЕРЖДЕН
на заседании кафедры
«15».06.2026г., протокол № 09
Заведующий кафедрой
_____ Э.Д. Алисултанова

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Управление персоналом при обеспечении информационной безопасности»

Направление подготовки

10.03.01 Информационная безопасность

Направленность (профиль)

«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Квалификация

бакалавр

Составитель _____ Л.К. Хаджиева

Грозный – 2026

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Управление персоналом при обеспечении информационной безопасности»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Предпосылки и основные направления развития менеджмента в сфере информационной безопасности	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет
2.	Международные организации в сфере информационной безопасности	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет
3.	Создание системы управления информационной безопасностью на предприятии	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет
4.	Основы построения политики информационной безопасности на предприятии	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
5.	Безопасность информационных технологий предприятия	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
6.	Департамент информационной безопасности предприятия и работа с персоналом	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Экзамен
7.	Аудит состояния информационной безопасности на предприятии	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет
8.	Программные средства, поддерживающие управление информационной	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация)

	безопасностью на предприятии		Зачет
9.	Организация реагирования на инциденты в сфере информационной безопасности	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет
10.	Предоставление услуг в сфере информационной безопасности	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет
11.	Управление информационной безопасностью на уровне крупных поставщиков информационных систем	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет
12.	Управление информационной безопасностью на государственном уровне	ПК-2; ПК-3	Лабораторные работы Доклады с презентациями Письм. контрольная работа (аттестация) Зачет

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1.	Лабораторная работа	Задания, выполняемые с использованием изучаемого программного обеспечения с целью углубления и закрепления теоретических знаний и развития навыков самостоятельного проведения эксперимента	Комплект заданий для выполнения лабораторных работ
2.	Доклад с презентацией	Продукт самостоятельной работы студента, представляющий собой публичное выступление по определенной учебно-практической, исследовательской или научной теме	Темы докладов
3.	Письм. контрольная работа (аттестация)	Подведение итогов учебной деятельности студентов в течение семестра в письменной форме	Вопросы по темам / разделам дисциплины
4.	Зачет	Итоговая форма оценки знаний	Вопросы к зачету

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

Лабораторные работы организуются в компьютерных аудиториях и выполняются по заданию преподавателя с использованием изучаемого программного обеспечения.

8 семестр

Лабораторная работа №1 Построение функциональной модели процессов обеспечения информационной безопасности с помощью графических нотаций.

Лабораторная работа №2 Нормативно-правовые документы и стандарты в области защиты информации и информационной безопасности

Лабораторная работа №3 Определение угроз безопасности информации в компьютерной системе организации

Лабораторная работа № 4 Анализ рынка и подбор средств для проекта СЗИ предприятия.

Лабораторная работа №5 Оценка рисков информационной безопасности компании на основе модели информационных потоков

Лабораторная работа №6 Изучение методов и средств обеспечения безопасности информационных и телекоммуникационных технологий

Лабораторная работа №7 Изучение методологии аудита информационной безопасности организации

Лабораторная работа №8 Контроль целостности программной среды.

Лабораторная работа №9 Определение потенциала нарушителя, необходимого для реализации угрозы безопасности информации

Лабораторная работа №10 Исследование предприятия по предоставлению услуг в сфере информационной безопасности

Лабораторная работа №11 Изучение системы правление информационной безопасностью

Лабораторная работа №12 Изучение государственных нормативных актов по управлению информационной безопасностью на государственном уровне

ТЕМЫ ДОКЛАДОВ С ПРЕЗЕНТАЦИЯМИ

Подготовка презентации на 12-15 слайдов с устным докладом по заданной тематике:

8семестр

Способ организации самостоятельной работы: подготовка презентации с устным докладом по заданной тематике.

1. Безопасность и правовое регулирование электронной коммерции
2. Обзор деятельности центров реагирования на инциденты в РФ
3. Обзор деятельности МСЭТ по управлению информационной безопасности
4. .Обзор материалов Гост Р ИСО/МЭК 18044 -2007 Менеджмент инцидентов информационной безопасности
5. Обзор материалов Гост ISO/IEC 27005-2012 Методы обеспечение безопасности. Менеджмент рисков безопасности
6. Менеджмент непрерывности бизнеса
7. Менеджмент оказание услуг третьим лицам и клиентам
8. Направления организационной работы в области безопасности, связанной с персоналом
9. Оценка эффективности передачи риска информационной безопасности третьим лицам
10. Мониторинг безопасности
11. Задачи департамента информационной безопасности
12. Аудит безопасности информационных технологий.

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д. МИЛЛИОНЩИКОВА

Институт прикладных информационных технологий

Кафедра Информатика и вычислительная техника

Вопросы к зачету (экзамену) по дисциплине «Управление персоналом при обеспечении информационной безопасности»

Итоговая отчетность студентов по дисциплине принимается по билетам, с предоставлением времени на подготовку (20-30 мин.) и последующим устным ответом преподавателю. Состав билета на экзамен / зачет – 1 теоретический вопрос, 1 задача.

8 семестр

Вопросы к зачету

К 1-ой рубежной аттестации:

1. Дайте понятие информационной безопасности в узком и широком смысле слова
2. Дайте определение рисков и охарактеризуйте их виды
3. Дайте определение угроз и охарактеризуйте их виды.
4. Охарактеризуйте основные наиболее распространенные способы нарушения информационной безопасности
5. Охарактеризуйте процесс обеспечения собственной информационной безопасности на предприятиях.
6. Укажите основные международные организации, действующие в сфере информационной безопасности и укажите решаемые ими задачи.
7. Опишите отличительные особенности крупных международных профессиональных (отраслевых) организаций (объединений).
8. Дайте определение системы управления информационной безопасностью (СУИБ) предприятия, приведите её состав и цели создания.
9. Основные этапы и условия разработки СУИБ.
10. Опишите организационную структуру менеджмента обеспечения информационной безопасности предприятия
11. Основные функции отдела информационной безопасности предприятия.
12. Сценарий анализа информационных рисков компании
13. Дайте определение и поясните смысл политики безопасности предприятия
14. Поясните основные этапы управления безопасностью информационных технологий.
15. Опишите процедуру оценки общего уровня риска при управлении безопасностью информационных технологий.
16. Дайте определение и раскройте задачи, решаемые департаментом информационной безопасности предприятия (ДИБП).
17. Опишите функции ДИБП, связанные с формированием, поддержкой и документальным обеспечением политики информационной безопасности предприятия.
18. Опишите функции ДИБП, с внедрением средств защиты информации.
19. Опишите функции ДИБП, связанные с администрированием информационных систем и систем защиты информации

20. Дайте определение аудита состояния информационной безопасности предприятия. Охарактеризуйте их виды.

21. Опишите цели и стратегическую задачу аудита состояния информационной безопасности предприятия.

22. Опишите требования к организациям, осуществляющим внешний аудит состояния информационной безопасности предприятия.

23. Основные этапы аудита состояния информационной безопасности предприятия и их характеристика

24. Охарактеризуйте процесс анализа действующей на предприятии политики безопасности.

25. Охарактеризуйте процесс изучения (проверки) действующих информационных ресурсов предприятия.

Ко 2-ой рубежной аттестации:

1. Виды программных средств поддержки реализации политики информационной безопасности.

2. Структура и краткое содержание отчета о состоянии информационной безопасности программного продукта «COBRA».

3. Дайте характеристику программного комплекса управления политикой информационной безопасности компании «КОНДОР+».

4. Предпосылки разработки политики безопасности предприятия.

5. Структура деятельности в сфере информационной безопасности. Основные задачи организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности

6. Что включает в себя безопасная информационная инфраструктура?

7. Иерархия уровней организационной работы в сфере информационной безопасности и их характеристика

8. Охарактеризуйте этап разработки СУИБ: Оценка информационных рисков

9. Охарактеризуйте этап разработки СУИБ: Внедрение выбранных мер обработки рисков

10. Охарактеризуйте этап разработки СУИБ: Контроль выполнения и эффективности выбранных мер.

11. Охарактеризуйте верхний уровень политики информационной безопасности предприятия

12. Охарактеризуйте средний уровень политики информационной безопасности предприятия

13. Приведите перечень основных вопросов, входящих в состав политики безопасности информационных технологий.

14. Опишите функции ДИБП, связанные с контролем выполнения требований политики информационной безопасности и проведением аудитов.

15. Инструментальная проверка защищенности информационной системы предприятия.

16. Анализ собранной информации при аудите состояния информационной безопасности предприятия.

17. Содержание заключения при аудите состояния информационной безопасности предприятия.

18. Назначение программных средства, реализующих методологии анализа рисков.

19. Опишите назначение и возможности семейства программных продуктов "CRAMM".

20. Назначение и основные функции программных средств, интегрируемых в информационную систему предприятия.

21. Перечислите и охарактеризуйте известные программные средства, интегрируемые в информационную систему предприятия.

22. Дайте характеристику услуги первичной постановки системы управления информационной безопасностью.

23. Страхование в сфере информационной безопасности и основные объекты страхования.

24. Общая политика России в сфере информационной безопасности

25. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

При оценке ответа студента на экзамене / зачете учитываются:

- правильность ответа на вопрос;
- логика изложения материала вопроса;
- правильность ответа на дополнительные вопросы;
- умение увязывать теоретические и практические аспекты вопроса;
- культура устной речи студента.

В пределах, допускаемых на экзамене / зачете 20 баллов студенту выставляется:

Более 15 баллов – студент показывает всестороннее глубокое систематическое знание учебно-методического материала, усвоил основную литературу и знаком с дополнительной литературой; самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы билета; умеет анализировать, классифицировать, обобщать и систематизировать изученный материал, устанавливать причинно-следственные связи; увязывает теоретические аспекты предмета с практическими задачами.

От 6 до 15 баллов – студент обнаруживает, в основном, полное знание учебно-программного материала, успешно выполняет предусмотренные в программе задания; излагает ответы на поставленные вопросы систематизированно и последовательно, но имеются пробелы знаний в некоторых разделах; демонстрирует умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; способен к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности.

До 5 баллов – студент показывает знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы, знаком с основной литературой, рекомендованной программой, однако проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов. Студент способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом практических навыков.

0 баллов – студент показывает существенные пробелы в знаниях основного учебного программного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий; не способен ответить на вопросы билета даже при дополнительных наводящих вопросах преподавателя.

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

«Управление персоналом при обеспечении информационной безопасности»

ЗАЧЕТНО-ЭКЗАМЕНАЦИОННЫЕ МАТЕРИАЛЫ

8 СЕМЕСТР, ЗАЧЕТ

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 1

1. Дайте определение аудита состояния информационной безопасности предприятия. Охарактеризуйте их виды.

2. Опишите организационную структуру менеджмента обеспечения информационной безопасности предприятия

3. Опишите функции ДИБП, связанные с контролем выполнения требований политики информационной безопасности и проведением аудитов.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 2

1. Дайте определение и раскройте задачи, решаемые департаментом информационной безопасности предприятия (ДИБП).

2. Опишите функции ДИБП, связанные с администрированием информационных систем и систем защиты информации

3. Дайте определение угроз и охарактеризуйте их виды.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 3

1. Опишите функции ДИБП, связанные с контролем выполнения требований политики информационной безопасности и проведением аудитов.

2. Основные функции отдела информационной безопасности предприятия.

3. Виды программных средств поддержки реализации политики информационной безопасности.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 4

1. Содержание заключения при аудите состояния информационной безопасности предприятия.

2. Перечислите и охарактеризуйте известные программные средства, интегрируемые в информационную систему предприятия.

3. Приведите перечень основных вопросов, входящих в состав политики безопасности информационных технологий.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 5

1. Дайте определение угроз и охарактеризуйте их виды.

2. Общая политика России в сфере информационной безопасности

3. Приведите перечень основных вопросов, входящих в состав политики безопасности информационных технологий.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 6

1. Опишите функции ДИБП, связанные с формированием, поддержкой и документальным обеспечением политики информационной безопасности предприятия.

2. Приведите перечень основных вопросов, входящих в состав политики безопасности информационных технологий.

3. Основные функции отдела информационной безопасности предприятия.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 7

1. Инструментальная проверка защищенности информационной системы предприятия.

2. Структура деятельности в сфере информационной безопасности. Основные задачи организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности

3. Дайте определение и раскройте задачи, решаемые департаментом информационной безопасности предприятия (ДИБП).

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 8

1. Что включает в себя безопасная информационная инфраструктура?

2. Охарактеризуйте этап разработки СУИБ: Внедрение выбранных мер обработки рисков

3. Охарактеризуйте этап разработки СУИБ: Оценка информационных рисков

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 9

1. Охарактеризуйте процесс изучения (проверки) действующих информационных ресурсов предприятия.

2. Перечислите и охарактеризуйте известные программные средства, интегрируемые в информационную систему предприятия.

3. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 10

1. Дайте определение рисков и охарактеризуйте их виды

2. Укажите основные международные организации, действующие в сфере информационной безопасности и укажите решаемые ими задачи.

3. Виды программных средств поддержки реализации политики информационной безопасности.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 11

1. Иерархия уровней организационной работы в сфере информационной безопасности и их характеристика

2. Охарактеризуйте верхний уровень политики информационной безопасности предприятия

3. Опишите функции ДИБП, связанные с администрированием информационных систем и систем защиты информации

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 12

1. Виды программных средств поддержки реализации политики информационной безопасности.

2. Содержание заключения при аудите состояния информационной безопасности предприятия.

3. Дайте определение системы управления информационной безопасностью (СУИБ) предприятия, приведите её состав и цели создания.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 13

1. Дайте определение и поясните смысл политики безопасности предприятия

2. Охарактеризуйте процесс обеспечения собственной информационной безопасности на предприятиях.

3. Дайте определение рисков и охарактеризуйте их виды

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 14

1. Охарактеризуйте средний уровень политики информационной безопасности предприятия

2. Охарактеризуйте верхний уровень политики информационной безопасности предприятия

3. Охарактеризуйте этап разработки СУИБ: Оценка информационных рисков

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 15

1. Охарактеризуйте процесс обеспечения собственной информационной безопасности на предприятиях.

2. Опишите функции ДИБП, связанные с формированием, поддержкой и документальным обеспечением политики информационной безопасности предприятия.

3. Дайте характеристику программного комплекса управления политикой информационной безопасности компании «КОНДОР+».

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 16

1. Опишите назначение и возможности семейства программных продуктов "CRAMM".

2. Основные функции отдела информационной безопасности предприятия.

3. Дайте понятие информационной безопасности в узком и широком смысле слова

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 17

1. Поясните основные этапы управления безопасностью информационных технологий.

2. Опишите процедуру оценки общего уровня риска при управлении безопасностью информационных технологий.

3. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 18

1. Опишите функции ДИБП, связанные с контролем выполнения требований политики информационной безопасности и проведением аудитов.

2. Укажите основные международные организации, действующие в сфере информационной безопасности и укажите решаемые ими задачи.

3. Охарактеризуйте процесс обеспечения собственной информационной безопасности на предприятиях.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 19

1. Основные этапы и условия разработки СУИБ.

2. Дайте определение аудита состояния информационной безопасности предприятия. Охарактеризуйте их виды.

3. Охарактеризуйте верхний уровень политики информационной безопасности предприятия

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт прикладных информационных технологий
Группа"" Семестр ""
Дисциплина "Управление персоналом при обеспечении информационной безопасности"
Билет № 20

1. Укажите основные международные организации, действующие в сфере информационной безопасности и укажите решаемые ими задачи.

2. Иерархия уровней организационной работы в сфере информационной безопасности и их характеристика

3. Дайте определение рисков и охарактеризуйте их виды

Подпись преподавателя_____ Подпись заведующего кафедрой_____