МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА»

Информатика и вычислительная техника

УТВЕРЖДЕН

на заседании кафедры
«17» 01 2024 г., протокол № 5

Заведующий кафедрой
_____ Э.Д. Алисултанова

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Анализ и оценка рисков информационной безопасности»

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль)
«Организация и технологии защиты информации»

Квалификация
бакалавр

Год начала подготовки – 2024

Составитель (и) _____ М.М. Намаева

Грозный – 2024

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Анализ и оценка рисков информационной безопасности»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Основные цели и терминология задач анализа рисков в системах информационной безопасности	ПК-1. ПК-1.1. ПК-1.2. ПК-1.3.	Опрос Билеты к рубежным аттестациям Билеты к зачету
2	Теоретические основы и модели анализа рисков	ПК-3. ПК-3.1. ПК 3.2. ПК 3.3.	Опрос Билеты к рубежным аттестациям Самостоятельная работа Билеты к зачету
3	Стандарты по анализу рисков в системах ИБ	ПК-3. ПК-3.1. ПК 3.2. ПК 3.3.	Опрос Билеты к рубежным аттестациям Билеты к зачету
4	Задачи анализа рисков в системах ИБ	ПК-1. ПК-1.1. ПК-1.2. ПК-1.3.	Тестирование Билеты к рубежным аттестациям Самостоятельная работа Билеты к зачету
5	Основы управления рисками в системах защиты информации	ПК-3. ПК-3.1. ПК 3.2. ПК 3.3.	Тестирование Билеты к рубежным аттестациям Билеты к зачету

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	*Лабораторная работа*	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом	Комплект заданий для выполнения лабораторных работ
2	*Экзамен*	Итоговая форма оценки знаний	Билеты к экзамену

Первый семестр
Вопросы к 1ой рубежной аттестации:

1. Понятие риска в различных сферах жизни общества.
2. Взаимосвязь основных понятий в области оценки рисков.
3. Понятие киберриска, угрозы, уязвимости, понятие и виды ущерба от атак, тотальный и остаточный риск, качественный и количественный риск, предпринимательский риск, цели анализа риска.
4. Классификации и характеристики рисков.
5. Место анализа рисков в общей схеме управления ИБ.
6. Подходы к оценке рисков ИБ: качественный, количественный.
7. Экономическая модель оценки рисков.
8. Вероятностная модель оценки рисков основная концепция анализа рисков в системах защиты информации.
9. Модели анализа риска.

Вопросы ко 2ой рубежной аттестации:

1. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 31000-2010.
2. Менеджмент риска. Принципы и руководство. ГОСТ Р ИСО 31010.
3. Методы оценки риска. Характеристика отечественных документов по анализу уровня защищенности объектов информатизации.
4. Характеристика зарубежных и международных стандартов.
5. Стандарты серии NIST SP 800, стандарты серии ISO/IEC, стандарт IEC 31010:2019.
6. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 27005.
7. Менеджмент рисков ИБ. Стандарт банка России по обеспечению ИБ организаций банковской системы РФ.
8. Оценка, измерение и прогнозирование рисков. Характеристика современных методик анализа рисков.
9. Методики: ГРИФ, FRAP, RiskWatch, CRAMM, OCTAVE.
10. Документы ФСТЭК по оценке защищенности объектов информатизации.
11. Методики и ПО для оценки рисков ИБ.
12. Метод анализа и управления рисками CRAMM.
13. Принятие решений по результатам оценки рисков.
14. Политика обработки рисков. Подведение итогов.
15. Основы минимизации рисков.

16. Избегание рисков, передача и принятие рисков, страхование и диверсификация производства.
17. Выбор методов и средств защиты информации на основе анализа рисков.

Образец типового задания для лабораторных занятий

Лабораторная работа №1. Организация консалтинговой компании

Цель работы: Познакомиться на практике с организационной структурой компании по проведению аудиту информационной безопасности предприятия.

Программно-аппаратные средства: компьютерная лаборатория, стандартные средства Microsoft Office.

Теоретическая часть:

Консалтинг — деятельность по консультированию производителей, продавцов, покупателей по широкому кругу вопросов в сфере технологической, технической, экспертной деятельности. Цель консалтинга — помочь менеджменту в достижении заявленных целей. Консалтинговые компании специализируются по отдельным направлениям деятельности (например, финансовом, организационном, стратегическом)

Основная задача консалтинга заключается в анализе, обосновании перспектив развития и использования научно-технических и организационно-экономических инноваций с учетом предметной области и проблем клиента. Иными словами, консалтинг - это любая помощь, оказываемая внешними консультантами, в решении той или иной проблемы.

Информационная безопасность (ИБ) некоторой ИС – это уровень ее защищенности от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, изменения или разрушения их компонентов.

Система защиты информации (СЗИ) – это система, обеспечивающая информационную безопасность некоторой ИС.

Аудит информационной безопасности – это системный процесс получения объективных качественных и количественных оценок текущего состояния информационной безопасности некоторой информационной системы, в соответствии с определенными критериями и показателями безопасности.

Конфиденциальность (Confidentiality of Information) – это свойство информации быть известной только допущенным пользователям ИС.

Целостность (Integrity of Information) – это свойство информации быть неизменной в семантическом отношении.

Доступность (Availability of Information) – это свойство информации быть

свободной на доступ в определенный момент времени.

Доступ к информации (Access to Information) – возможность ознакомления с информацией, ее обработка. Например, чтение, копирование, модификация или уничтожение информации.

Целостность, конфиденциальность и доступность ресурсов ИС вполне возможно измерять, например, на качественных шкалах, привлекая экспертов.

Круг проблем, решаемых консалтингом, весьма широк, кроме того, специализация компаний, предоставляющих консалтинговые услуги, может быть различной: от узкой, ограничивающейся каким-либо одним направлением консалтинговых услуг (например, аудит), до самой широкой, охватывающей полный спектр услуг в этой области. Соответственно этому, каждый специалист (или каждая фирма), работающая в данной области, вкладываете понятие консалтинга собственный смысл и придает ему собственный оттенок, определяемый направлением деятельности конкретной компании.

Итак, Консалтинг - это вид интеллектуальной деятельности, основная задача которого заключается в анализе, обосновании перспектив развития и использования научно-технических и организационно-экономических инноваций с учетом предметной области и проблем клиента.

Консалтинг решает вопросы управленческой, экономической, финансовой, инвестиционной деятельности организаций, стратегического планирования, оптимизации общего функционирования компании, ведения бизнеса, исследования и прогнозирования рынков сбыта, движения цен и т.д. Иными словами, консалтинг - это любая помощь, оказываемая внешними консультантами, в решении той или иной проблемы.

Основная цель консалтинга заключается в улучшении качества руководства, повышении эффективности деятельности компании в целом и увеличении индивидуальной производительности труда каждого работника.

Согласно распространенному мнению, к услугам внешних консультантов обращаются в основном и в первую очередь те организации, которые оказались в критическом положении. Однако помощь в критических ситуациях - отнюдь не основная функция консалтинга.

Контрольные вопросы

1. Что такое консалтинг?
2. Какова основная задача консалтинга?
3. Что понимают под информационной безопасностью?
4. Что представляет собой система защиты информации?
5. Что понимают под аудитом ИБ?

6. Перечислите основные свойства информации.
7. Каковы способы измерения свойств информации?

Задание

1. Изучить основной теоретический материал
2. Создать структурную модель консалтинговой компании.
3. Провести организационные мероприятия по подготовке проведения аудита.
4. Уточнить цели и задачи аудита
5. Сформировать рабочую группу
6. Подготавливается и согласовывается техническое задание на проведение аудита компании (по вариантам).
7. Собирать информацию и дать оценку следующих мер и средств:

- организационных мер в области информационной безопасности;
- программно-технических средств защиты информации;
- обеспечения физической безопасности.

Отчет по лабораторной работе № 1

Название работы

Расчет рисков информационной безопасности.

Цель

Познакомиться на практике с методом расчета рисков ИБ на основе модели анализа угроз и уязвимостей от Digital Security.

Выполнил

Студент гр. № _____

ФИО _____

Отчет

1. Структура и описание консалтинговой компании.
2. Перечень услуг консалтинговой компании.
3. Состав рабочей группы:
4. Цели и задачи аудита ИБ:
5. Техническое задание:
6. Придумать или использовать реальную ИС некоторой организации (по вариантам).
7. Исходные данные о заказчике:
8. Выводы по результатам анализа исходных данных от заказчика
9. Ответы на контрольные вопросы.

Критерии оценки ответов на лабораторные работы:

- не зачтено выставляется студенту, если *дан неполный ответ*, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

- зачтено выставляется студенту, если *дан полный, развернутый ответ* на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей.* Ответ изложен литературным языком в терминах науки. *Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.*

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт прикладных информационных технологий

Кафедра Информатика и вычислительная техника

Вопросы к экзамену по дисциплине
«Анализ и оценка рисков информационной безопасности»

1. Основные понятия защиты информации и информационной безопасности
2. Понятие риска в различных сферах жизни общества.
3. Взаимосвязь основных понятий в области оценки рисков.
4. Понятие киберриска, угрозы, уязвимости, понятие и виды ущерба от атак, тотальный и остаточный риск, качественный и количественный риск, предпринимательский риск, цели анализа риска.
5. Классификации и характеристики рисков.
6. Место анализа рисков в общей схеме управления ИБ.
7. Подходы к оценке рисков ИБ: качественный, количественный.
8. Экономическая модель оценки рисков.
9. Вероятностная модель оценки рисков основная концепция анализа рисков в системах защиты информации.
10. Модели анализа риска.
18. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 31000-2010.
19. Менеджмент риска. Принципы и руководство. ГОСТ Р ИСО 31010.
20. Методы оценки риска. Характеристика отечественных документов по анализу уровня защищенности объектов информатизации.
21. Характеристика зарубежных и международных стандартов.
22. Стандарты серии NIST SP 800, стандарты серии ISO/IEC, стандарт IEC 31010:2019.

23. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 27005.
24. Менеджмент рисков ИБ. Стандарт банка России по обеспечению ИБ организаций банковской системы РФ.
25. Оценка, измерение и прогнозирование рисков. Характеристика современных методик анализа рисков.
26. Методики: ГРИФ, FRAP, RiskWatch, CRAMM, OCTAVE.
27. Документы ФСТЭК по оценке защищенности объектов информатизации.
28. Методики и ПО для оценки рисков ИБ.
29. Метод анализа и управления рисками CRAMM.
30. Принятие решений по результатам оценки рисков.
31. Политика обработки рисков. Подведение итогов.
32. Основы минимизации рисков.
33. Избегание рисков, передача и принятие рисков, страхование и диверсификация производства.
34. Выбор методов и средств защиты информации на основе анализа рисков.

Критерии оценки знаний студента на экзамене

Оценка «отлично» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка «хорошо» - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка «удовлетворительно» - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «неудовлетворительно» - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

Приложение 3

Экзаменационные билеты

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени академика М.Д. Миллионщикова

БИЛЕТ № 1

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Основные понятия защиты информации и информационной безопасности.
2. Выбор методов и средств защиты информации на основе анализа рисков.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Э.Д. Алисултанова

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени академика М.Д. Миллионщикова

БИЛЕТ № 2

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Понятие риска в различных сферах жизни общества.
2. Избегание рисков, передача и принятие рисков, страхование и диверсификация производства.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 3

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Взаимосвязь основных понятий в области оценки рисков.
2. Основы минимизации рисков.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 4

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Понятие киберриска, угрозы, уязвимости, понятие и виды ущерба от атак, тотальный и остаточный риск, качественный и количественный риск, предпринимательский риск, цели анализа риска.
2. Политика обработки рисков. Подведение итогов

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 5

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. . Классификации и характеристики рисков.
2. Принятие решений по результатам оценки рисков.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 6

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Место анализа рисков в общей схеме управления ИБ.
2. Метод анализа и управления рисками CRAMM.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 7

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Подходы к оценке рисков ИБ: качественный, количественный.
2. Методики и ПО для оценки рисков ИБ.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 8

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Экономическая модель оценки рисков.
2. Документы ФСТЭК по оценке защищенности объектов информатизации.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 9

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Вероятностная модель оценки рисков основная концепция анализа рисков в системах защиты информации.
2. Методики: ГРИФ, FRAP, RiskWatch, CRAMM, OCTAVE.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 10

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Модели анализа риска.
2. Оценка, измерение и прогнозирование рисков. Характеристика современных методик анализа рисков.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 11

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 31000-2010.
2. Менеджмент рисков ИБ. Стандарт банка России по обеспечению ИБ организаций банковской системы РФ.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 12

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Менеджмент риска. Принципы и руководство. ГОСТ Р ИСО 31010.
2. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 27005.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 13

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Методы оценки риска. Характеристика отечественных документов по анализу уровня защищенности объектов информатизации.
2. Стандарты серии NIST SP 800, стандарты серии ISO/IEC, стандарт IEC 31010:2019.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 14

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Характеристика зарубежных и международных стандартов.
2. Выбор методов и средств защиты информации на основе анализа рисков.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 15

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Основные понятия защиты информации и информационной безопасности
2. Избегание рисков, передача и принятие рисков, страхование и диверсификация производства.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 16

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Понятие риска в различных сферах жизни общества.
2. Основы минимизации рисков.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 17

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Взаимосвязь основных понятий в области оценки рисков.
2. Политика обработки рисков. Подведение итогов.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 18

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Модели анализа риска.
2. Принятие решений по результатам оценки рисков.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 19

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Классификации и характеристики рисков.
2. Метод анализа и управления рисками CRAMM.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова

БИЛЕТ № 20

Дисциплина ***«Анализ и оценка рисков информационной безопасности»***
Институт прикладных информационных технологий
Кафедра *«Информатика и вычислительная техника»*

1. Место анализа рисков в общей схеме управления ИБ.
2. Методики и ПО для оценки рисков ИБ.

УТВЕРЖДЕНО зав. кафедрой

на заседании кафедры

протокол № ___ от _____ _____ Э.Д. Алисултанова