ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утверждены решением
Ученого совета ДГУНХ,
протокол № 11
от 06 июня 2023 г.

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПО ДИСЦИПЛИНЕ
«Анализ рисков и аудит информационной безопасности автоматизированных систем»

НАПРАВЛЕНИЕ ПОДГОТОВКИ – 10.04.01
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПРОФИЛЬ
«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ»

Уровень высшего образования - магистратура

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00DDAA21EB96DCD5ECDD494784A037C099
Владелец: Бучаев Ахмед Гамидович
Действителен: с 28.04.2023 до 21.07.2024

Махачкала – 2023

УДК 681.518(075.8)
ББК 32.81.73

Составитель – Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры "Математические методы в экономике" Дагестанского государственного университета.

Представитель работодателя - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

Оценочные материалы по дисциплине «Анализ рисков и аудит информационной безопасности автоматизированных систем» разработаны в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 26 ноября 2020 г., № 1455, в соответствии с приказом Министерства науки и высшего образования от 6.04.2021 г., № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам магистратуры, программам специалитета, программам магистратуры»

Оценочные материалы по дисциплине «Анализ рисков и аудит информационной безопасности автоматизированных систем» размещены на официальном сайте www.dgunh.ru

Гасанова З.А. Оценочные материалы по дисциплине «Анализ рисков и аудит информационной безопасности автоматизированных систем» для направления подготовки 10.04.01 Информационная безопасность, профиль «Управление информационной безопасностью и технологии защиты информации». – Махачкала: ДГУНХ, 2023 г. – 40 с.

Рекомендованы к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендованы к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрены на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 г., протокол № 10.

СОДЕРЖАНИЕ

Назначение оценочных материалов

Оценочные материалы для текущего контроля успеваемости (оценивания хода освоения дисциплин), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по дисциплине) обучающихся по дисциплине «Анализ рисков и аудит информационной безопасности автоматизированных систем» на соответствие их учебных достижений поэтапным требованиям образовательной программы высшего образования 10.04.01 Информационная безопасность, профиль «Управление информационной безопасностью и технологии защиты информации»

Оценочные материалы по дисциплине «Анализ рисков и аудит информационной безопасности автоматизированных систем» включают в себя: перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОПОП; методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Оценочные материалы сформированы на основе ключевых принципов оценивания:

- валидности: объекты оценки должны соответствовать поставленным целям обучения;
- надежности: использование единообразных стандартов и критериев для оценивания достижений;
- объективности: разные обучающиеся должны иметь равные возможности для достижения успеха.

Основными параметрами и свойствами оценочных материалов являются:

- предметная направленность (соответствие предмету изучения конкретной дисциплины);
- содержание (состав и взаимосвязь структурных единиц, образующих содержание теоретической и практической составляющих дисциплины);
- объем (количественный состав оценочных материалов);
- качество оценочных материалов в целом, обеспечивающее получение объективных и достоверных результатов при проведении контроля с различными целями.

РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины

1.1 Перечень формируемых компетенций

код компетенции	формулировка компетенции
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-2	Способен осуществлять сбор, анализ и систематизацию научно-технической информации по вопросам обеспечения информационной безопасности объектов информатизации

1.2. Перечень компетенций с указанием видов оценочных средств

Формируемые компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
ПК-2. Способен осуществлять сбор, анализ и систематизацию научно-технической информации по вопросам обеспечения информационной безопасности объектов информатизации	ИПК-2.1. Проводит анализ безопасности объектов информатизации	**Знать:** - методы аудита подсистем обеспечения безопасности средств защиты информации; - методы анализа защищенности автоматизированных систем	Пороговый уровень	Обучающийся слабо (частично) знает методы аудита подсистем обеспечения безопасности средств защиты информации; методы анализа защищенности автоматизированных систем	**Блок А –** задания репродуктивного уровня – тестовые задания; – вопросы для устного опроса
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает методы аудита подсистем обеспечения безопасности средств защиты информации;	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				методы анализа защищенности автоматизированных систем	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает методы аудита подсистем обеспечения безопасности средств защиты информации; методы анализа защищенности автоматизированных систем ИБ	
		Уметь: - проводить анализ защищенности отельных подсистем средств защиты информации	Пороговый уровень	Обучающийся слабо (частично) умеет проводить анализ защищенности отельных подсистем средств защиты информации	**Блок В** – задания реконструктивного уровня – письменная работа - тематика рефератов; - тематика презентаций;
			Базовый уровень	Обучающийся с незначительными затруднениями умеет проводить анализ защищенности отельных подсистем средств защиты информации	
			Продвинутый уровень	Обучающийся умеет проводить анализ защищенности отельных подсистем	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				средств защиты информации	
		Владеть: – навыками тестирования подсистем обеспечения безопасности средств защиты информации	Пороговый уровень	Обучающийся слабо (частично) владеет навыками тестирования подсистем обеспечения безопасности средств защиты информации	**Блок С** – задания практико-ориентированного уровня - проект; - кейсы; - деловая игра.
			Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками тестирования подсистем обеспечения безопасности средств защиты информации	
			Продвинутый уровень	Обучающийся свободно владеет навыками тестирования подсистем обеспечения безопасности средств защиты информации	
	ИПК-2.2. Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты	**Знать:** - процессы, процедуры, методы оценки рисков информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) знает процессы, процедуры, методы оценки рисков информационной безопасности.	**Блок А –** задания репродуктивного уровня – тестовые задания; – вопросы для устного опроса
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
	информации и экспертизу состояния защищенности информации с использованием современного инструментария и интеллектуальных информационно-аналитических систем			пробелами знает процессы, процедуры, методы оценки рисков информационной безопасности.	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает процессы, процедуры, методы оценки рисков информационной безопасности.	
		Уметь: - определять и обосновывать активы, ресурсы, роли, деятельности для процессов и процедур управления информационной безопасности защищённых автоматизированных систем	Пороговый уровень	Обучающийся слабо (частично) умеет определять и обосновывать активы, ресурсы, роли, деятельности для процессов и процедур управления информационной безопасности защищённых автоматизированных систем**.**	**Блок В** – задания реконструктивного уровня – тематика рефератов; - тематика презентаций; - практическая работа.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет определять и обосновывать активы, ресурсы, роли, деятельности для процессов и процедур управления информационной	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				безопасности защищённых автоматизированных систем	
			Продвинутый уровень	Обучающийся умеет определять и обосновывать активы, ресурсы, роли, деятельности для процессов и процедур управления информационной безопасности защищённых автоматизированных систем	
		Владеть: - навыками расчета рисков информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) владеет навыками расчета рисков информационной безопасности	**Блок С** – задания практико-ориентированного уровня - кейсы; - практическая работа.
			Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками расчета рисков информационной безопасности	
			Продвинутый уровень	Обучающийся свободно владеет навыками расчета рисков информационной безопасности	

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине

Для проверки сформированности компетенции ПК-2. Способен осуществлять сбор, анализ и систематизацию научно-технической информации по вопросам обеспечения информационной безопасности объектов информатизации

ИПК-2.1. Проводит анализ безопасности объектов информатизации
Блок А. Задания репродуктивного уровня («знать»)

А.1 Тестовые задания по дисциплине

1. Сколько уровне Политики безопасности выделяют?
   а) 3
   б) 4
   в) 5
   г) 2
2. Что такое политики безопасности?
   а) Пошаговые инструкции по выполнению задач безопасности
   б) Общие руководящие требования по достижению определенного уровня безопасности
   в) Широкие, высокоуровневые заявления руководства
   г) Детализированные документы по обработке инцидентов безопасности
3. Укажите последовательность этапов жизненного цикла политики безопасности:

3	Контроль выполнения требований ПБ
4	Разработка ПБ
1	Внедрение ПБ
2	Анализ и планирование внедрения ПБ

4. Что такое процедура?
   а) Правила использования программного и аппаратного обеспечения в компании
   б) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
   в) Пошаговая инструкция по выполнению задачи
   г) Обязательные действия
5. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
   а) Поддержка высшего руководства
   б) Актуальные и адекватные политики и процедуры безопасности
   в) Эффективные защитные меры и методы их внедрения

г) Проведение тренингов по безопасности для всех сотрудников

6. Сколько существует уровней организационной работы в сфере информационной безопасности?

а) 3
б) 4
в) 5
г) 2

7. Основными задачами государственного уровня организационной работы в сфере информационной безопасности являются:

а) Защита собственных информационных ресурсов
б) Разработка правил и стандартов, имеющих глобальное значение
в) Методологическая и организационная поддержка использования продуктов и услуг, поставляемых на рынок
г) Регулирование использования ИС и распространения информации с целью недопущения противоправных действий, ущерба другим участникам информационного обмена

8. Какой из стандартов определяет нормы и правила менеджмента информационной безопасности?

д) ISO/IEC 27002
е) ISO/IEC 27001
ж) ISO/IEC 18044
з) ГОСТ 28147-89

9. Какой из стандартов определяет модель разработки и функционирования СМИБ?

д) ISO/IEC 27002
е) ISO/IEC 27001
ж) ISO/IEC 18044
з) ГОСТ 28147-89

10. Какие виды аудитов ИБ выделяют?

а) Временный и постоянный
б) Внешний и внутренний
в) Безопасный и небезопасный
г) Организационный и технический

11. Что не может быть объектом проведения аудита безопасности?

а) Фирма
б) отдельные здания и помещения
в) отдельные системы или их компоненты
г) отдельные виды деятельности
д) персонал

12. На каком этапе менеджмента инцидентами осуществляется обобщение накопленного опыта и определение методом улучшения безопасности?

а) использование
б) анализ
в) улучшение

г) планирование и подготовка

А2. Вопросы для устного опроса

1. Структура и содержание Политики ИБ.
2. Источники информации для разработки Политики ИБ.
3. Особенности корпоративных и частных Политик ИБ.
4. Жизненный цикл Политики ИБ.
5. Ответственность за выполнение Политики ИБ.
6. Сущность и функции управления. Принципы, подходы и виды управления.
7. Понятие системы управления информационной безопасностью (СУИБ). Цели и задачи управления информационной безопасностью.
8. Стратегии построения и внедрения СУИБ в организации.
9. Циклическая модель PDCA.
10. ГОСТ 270 01.
11. Использование процессного подхода при управлении ИБ организации.
12. Этапы аудита
13. Концептуальная модель аудита
14. Методы анализа данных при аудите ИБ

Блок В. Задания реконструктивного уровня («уметь»)

В1. Письменная работа

Тема: Обеспечение защиты информации при работе с кадрами.

2.1. Составьте профили требований (профессиограммы) двух сотрудников вашей фирмы (начальник производственного отдела и работник службы безопасности).

2.2. Укажите основные мероприятия и процедуры профотбора, проводимые службами Вашей фирмы в каждом случае.

2.3. Сделайте выбор тестов (из предложенного набора), которые будут использоваться для проверки каждого из кандидатов.

2.4. Опишите процедуру увольнения прежних работников и связанные с ней действия администрации.

В2. Тематика рефератов

1. Корпоративная политика безопасности
2. Базовые принципы, лежащие в основе моделей политики безопасности в компьютерной системе
3. Частные политики безопасности
4. Политики безопасности компьютерных информационных систем
5. Аудит информационной безопасности.
6. Роль информационной безопасности в сфере электронной торговли

7. Комплексный подход к созданию системы защиты информации на предприятии.
8. Международная информационная безопасность.
9. Защита информационной среды на предприятии.
10. Обеспечение безопасного доступа к информационным ресурсам организации.
11. Комплексная информационная безопасность объекта.

В3. Тематика презентаций

1. Корпоративная политика безопасности
2. Базовые принципы, лежащие в основе моделей политики безопасности в компьютерной системе
3. Частные политики безопасности
4. Политики безопасности компьютерных информационных систем

5. Аудит информационной безопасности.
6. Роль информационной безопасности в сфере электронной торговли
7. Комплексный подход к созданию системы защиты информации на предприятии.
8. Международная информационная безопасность.
9. Защита информационной среды на предприятии.
10. Обеспечение безопасного доступа к информационным ресурсам организации.
11. Комплексная информационная безопасность объекта.

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С.1. Проектная работа

Практическая работа (проект)

Тема проекта: Требования, предъявляемые к Политике первого уровня

Политика информационной безопасности организации - высокоуровневый документ, описывающий основные принципы и правила, направленные на защиту информационных ресурсов организации.

Цель выполнения проекта заключается в формировании профессиональных компетенций обучаемых, выражающихся в способности проводить анализ документации на соответствие предъявляемым требованиям.

Задание.

1. Ознакомить с предоставленными преподавателем Политиками верхнего уровня организаций различных сфер деятельности.

2. Оценить по пятибалльной шкале содержание каждого из документов по следующим пунктам:
   - Определение ИБ в терминах деятельности данной организации, области действия политики, целей, задач и принципов ОИБ организации.
   - Изложение намерения ОИБ, направленного па достижение указанных целей и на реализацию принципов ОИБ.
   - Общие сведения об активах, подлежащих защите, их классификацию.
   - Модели угроз и нарушителей (внутреннего и внешнего) ИБ, на противодействие которым ориентирована корпоративная ПолИБ.
   - Высокоуровневое изложение правил и требований по ОИБ, представляющих особую важность для организации (например, обеспечение соответствия законодательным актам, нормативным документам РФ в области ОИБ и нормативным актам организации; требования к управлению ИБ; требования по предотвращению и обнаружению компьютерных вирусов и другого вредоносного ПО; требования по УНБ).
   - Санкции и последствия нарушений корпоративной ПолИБ.
   - Определение общих ролей и обязанностей, связанных с ОИБ, включая информирование об инцидентах ИБ.
   - Перечень частных ПолИБ, развивающих и детализирующих положения корпоративной Пол ИБ, а также указание подразделений организации, ответственных за их соблюдение и/или реализацию.
   - Положения по контролю реализации корпоративной ПолИБ организации.
   - Ответственность за реализацию и поддержку документа.
   - Условия пересмотра (выпуска новой редакции) документа.
3. Подготовить презентацию выполненного проекта.

Результат проекта. Результаты проекта представляют собой проекты Политики безопасности организации 1-го уровня и частной политики безопасности, а также презентация, отражающая основные этапы выполнения задания.

Проект «Разработка политики безопасности»

Политика информационной безопасности организации - высокоуровневый документ, описывающий основные принципы и правила, направленные на защиту информационных ресурсов организации.

Цель выполнения проекта заключается в формировании профессиональных компетенций обучаемых, выражающихся в способности участвовать в работах по разработке и реализации политики информационной безопасности.

Задание.

1. Проанализировать информационные процессы выбранной Вами организации и выявить критически важную информацию, которую необходимо защищать.
2. Разработать политику безопасности 1-го уровня организации в соответствии с требованиями нормативных документов.
3. Разработать частную политику безопасности. Объект политики выбирается исходя из специфики деятельности организации.
4. Подготовить презентацию выполненного проекта.

Результат проекта. Результаты проекта представляют собой проекты Политики безопасности организации 1-го уровня и частной политики безопасности, а также презентация, отражающая основные этапы выполнения задания.

Примерный перечень организаций

Номер варианта	**Организация**	**Метод оценки риска**
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
10	Дизайнерская фирма	2
11	Офис интернет-провайдера	3
13	Компания по разработке ПО для сторонних организаций	1
14	Агентство недвижимости	2
15	Туристическое агентство	3
16	Офис благотворительного фонда	4
19	Рекламное агентство	3
20	Отделение налоговой службы	4
21	Офис нотариуса	1
26	Гостиница	2

27	Праздничное агентство	3
29	Диспетчерская служба такси	1
30	Железнодорожная касса	2

С2. Решение кейсов

Задание 2. Кейс

Исходная ситуация:

В коммерческой организации, которая занимается поставками компьютерной техники для государственных и муниципальных органов. При сумме потенциального контракта (поставки) более 100 тысяч рублей данная компания должна участвовать в тендере, соответственно сталкиваться с конкурентной борьбой во время проведения торгов. Компания не имеет никаких внутренних документов, касающихся информационной безопасности, в том числе политики безопасности.

В процессе участия в одной из процедур торгов ответственный менеджер по торгам получает на корпоративную почту письмо с заголовком "Срочно. Документы" с неизвестного адреса. Данное письмо содержит единственный архивный файл без текста самого письма. Менеджер открывает архив, после чего автоматически запускается вирус, который не только блокирует рабочий компьютер с установленным программным обеспечением для торгов и авторизированной электронной подписью организации, но и пытается распространяться по внутренней сети компании.

Сотрудники ИТ-отдела реагируют достаточно оперативно, локализуют распространение вируса, устраняют сам вирус и последствия его действия на всех зараженных компьютерах в течение 3-х часов. Но за это время торги закрываются, и компания упускает крупный контракт (порядка миллиона рублей).

Кто, по Вашему мнению, виноват в данной ситуации (менеджер, который открывал неизвестное письмо; сотрудники ИТ-отдела, которые не предприняли превентивных мер)? Кого следует наказать?

С3. Деловая игра

Деловая игра «Аудит и управление инцидентами информационной безопасности»

Структура деловой игры.

Рассмотрим игровую модель как основную при разработке деловой игры. Игровая модель представляет собой совокупность следующих компонентов:

- цели игры;
- комплекс ролей и функций игроков;

- сценарий игры;
- правила игры.

Цель игры заключается в формировании профессиональных компетенций обучаемых, выражающихся в готовности к формированию, организации и поддержке выполнения комплекса мер по обеспечению информационной безопасности автоматизированных систем.

Комплекс ролей и функций участников игры (Рис. 1).

- *руководитель* – преподаватель, ведущий курс, осуществляет общее руководство проведением игры, готовит разбор и подведение итогов игры;
- *помощники руководителя* – (1-2 человека) ассистенты, лаборанты, которые контролируют действия всех категорий игроков, готовят исходные данные для разбора и подведения итогов;
- *пользователи (обычные)* АИС компании (1-2 человека) - выполняют операции, характерные для нормальной служебной деятельности сотрудников организации;
- *нарушители* политик и правил работы в АИС компании (1-2 человека), выполняющие действия или работы, представляющие собой факты нарушения режима и правил безопасности в АИС;
- *удаленные пользователи* (1-2 человека), выполняют операции, характерные для деятельности клиента компании;
- *внешние злоумышленники (хакеры)* (1 человек), выполняют действия злоумышленного характера по отношению к безопасности ресурсов АИС;
- *администраторы* DLP-системы - (2 - 3 человека), осуществляющие операции по настройке компонентов системы, а также по сбору и обработке информации о событиях в АИС компании. В сущности это, так называемые, по сложившейся в последнее десятилетие терминологии в области информационной безопасности *офицеры безопасности* ;
- *руководство компании* - (1 - 2 человека), выполняющие работы по управлению режимом информационной безопасности компании на основе информации о событиях в АИС, предоставляемых администраторами DLP-системы.

Сценарий игры:

В информационной системе коммерческого предприятия ООО «Рога и копыта», занимающегося оптовой продажей продуктов питания сетевым магазинам, развернута DLP-система с целью мониторинга поведения пользователей при использовании его информационных активов.

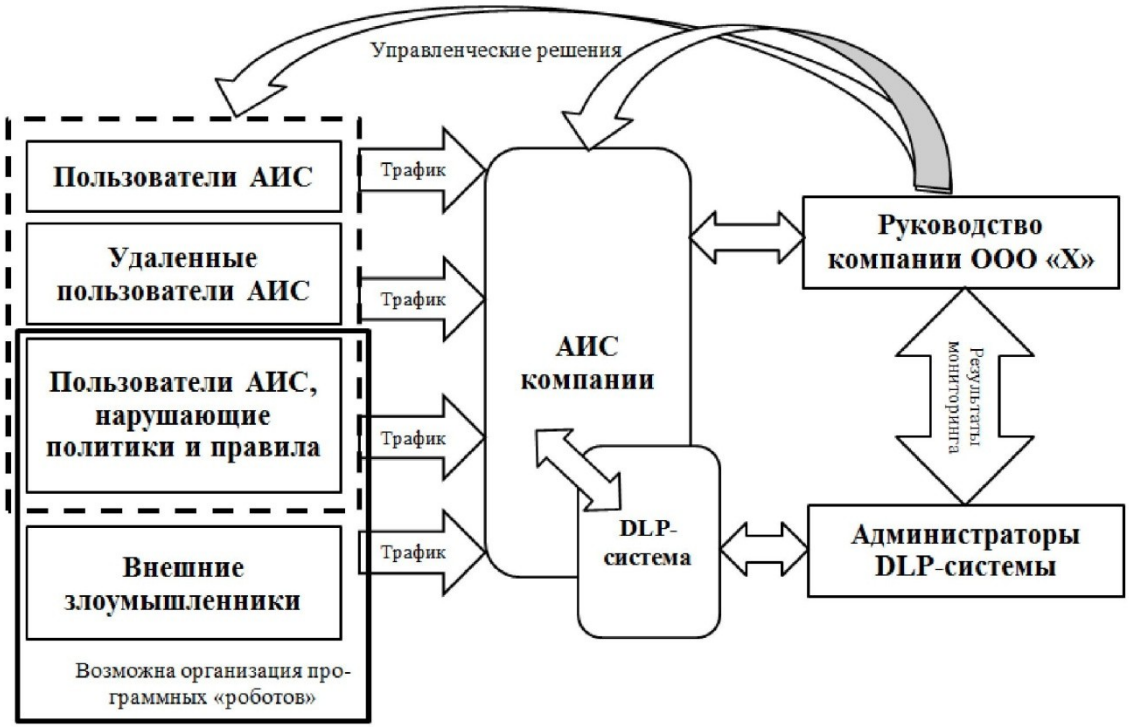

Рисунок 2. Распределение ролей участников игры и организация взаимодействия между ними

DLP-система «Контур информационной безопасности SearchInform» развернута в связи с имеющимися фактами нарушений порядка и правил использования информационных активов предприятия, описанных в политиках безопасности.

Частной политикой мониторинга действий пользователей в АИС организации администратору DLP-системы предписано предоставлять руководству результаты анализа сведений о событиях в системе не реже 1 раза в неделю, а при возникновении инцидентов ИБ или грубых нарушений – немедленно. При этом руководством вырабатываются управленческие решения, направленные на:

- АИС организации с целью совершенствования механизмов контроля и защиты ее информационных активов;
- сотрудников организации различных категорий по привитию им культуры поведения при работе в АИС и культуры информационной безопасности;
- управлению инцидентами информационной безопасности и проведению служебных расследований, связанных с ними.

Правила игры:

- Обучающиеся самостоятельно осуществляют распределение группы (подгруппы) по ролям;
- преподаватель выдает обучаемым общие материалы, групповые или индивидуальные задания и контролирует их подготовку;
- осуществляет контроль за действиями обучаемых в процессе игры;

- оценивает действия обучаемых в соответствии с принятыми критериями, т.е. является экспертом;
- подводит итоги игры.

Технология деловой игры состоит из следующих этапов.

Этап подготовки. Разработка игровой модели.

Этап ввода в игру. Данный этап заключается в ориентации всех категорий участников. Определяется режим работы, осуществляется постановка проблемы. Обучаемым выдаются материалы для подготовки. Осуществляется (при необходимости) сбор дополнительной информации. При необходимости обучаемые обращаются к руководителю игры за консультацией.

В процессе данного этапа допускаются предварительные контакты между участниками игры. Однако правилами игры запрещается следующее:

- отказываться от полученной, по решению руководителя, роли;
- самостоятельно выходить из игры;
- пассивно относиться к игре, подавлять активность, нарушать этику поведения.

Этап проведения – это непосредственно сам процесс игры, который должен сопровождаться обязательным выполнением некоторых правил:

- с началом игры никто не имеет права вмешиваться в нее и изменять ее ход;
- преподаватель имеет право корректировки действия участников игры только в тех случаях, когда участники уходят от главной цели игры.

Реализация сценария игры осуществляется следующим образом.

Все участники занимают места в двух учебных аудиториях. Участники игры, которые выполняют роли нарушителей, располагаются в отдельной аудитории, так как им предстоит выполнять специфические действия, имитирующие действия нарушителей (злоумышленников).

Участники игры, выполняющие роли сотрудников организации и удаленных пользователей АИС, выполняют задания в соответствии с их ролями. Результатом выполнения является трафик событий в АИС ООО «Рога и копыта», параметры которого поступают на вход DLP-системы. При этом участники выполняют свои задания с таким расчетом, чтобы с учебными и познавательными целями задействовать как можно больше ресурсов DLP-системы:

- редактируют документы;
- отправляют документы на печать и по электронной почте;
- пользуются ресурсами и сервисами интернет (http, ftp);
- подключают и используют в работе мобильные устройства типа съемных дисков, смартфонов, планшетов и др.;
- организуют между собой и с руководством компании общение с использованием службы немедленных сообщений, skype и подобных.

К этому трафику «подмешивается» информация о событиях, которые по своему содержанию представляют факты нарушений политики безопасности. Это может быть:

- посещение интернет-сайтов, содержание которых не связано с

исполняемыми сотрудниками должностными обязанностями;

- пересылка по электронной почте сообщений, содержащих «контролируемые» выражения;
- отправка на печать документов с грифом «Коммерческая тайна»;
- копирование документов с грифом «Коммерческая тайна» на мобильные носители;
- использование в процессе общения с применением служб мгновенных сообщений, skype и подобных «контролируемых» выражений, и другие.

В период, когда вышеперечисленные игроки занимаются «нагоном» трафика, администраторы DLP-системы выполняют следующие виды работ:

- проверяют работоспособность серверной и клиентских частей DLP-системы «**Контур информационной безопасности SearchInform**»;
- контролируют перечень активных компонентов системы и соответствие их параметров и настроенных реакций требованиям политики безопасности организации;
- администрируют серверную часть системы;
- контролируют работу модуля управления «Alert Center»;
- обрабатывают результаты мониторинга событий и выделяют из них те, которые имеют признаки относящихся к инцидентам безопасности;
- представляют выделенные события группе руководителей с заданной руководителем игры периодичностью (15-20 минут) исходя из продолжительности занятия.

В этот же период времени игроки группы руководителей выполняют следующие работы:

- руководят деятельностью администраторов;
- получают с заданной периодичностью результаты мониторинга;
- оценивают характер выделенных событий, заслуживающих немедленного реагирования;
- совместно с администраторами системы проводят анализ событий с целью определения признаков инцидентов;
- по выделенным инцидентам, а также в случае подозрения на таковые проводят работу с подчиненными из групп игроков: с сотрудниками организации, находящимися в аудитории 1 - непосредственным общением; с удаленными сотрудниками – по электронной почте и с использованием других средств. Если установлено, что выявленные инциденты или их признаки связаны с деятельностью внешних злоумышленников, то руководители вместе с администраторами (офицерами безопасности) вырабатывают контрмеры по минимизации последствий злоумышленных воздействий на функционирование АИС организации.

Подведение итогов деловой игры.

Каждая группа игроков к подведению итогов готовит отчет об участии в игре и достигнутых результатах, и самостоятельно (в случае недостаточной самостоятельности студентов – с помощью руководителя или помощника) выбирает одного из участников для выступления.

В процессе подведения итогов проводится заслушивание одного студента из каждой группы игроков. В процессе заслушивания студент докладывает результаты своего участия в игре по следующим позициям:

- характер выполняемой роли;
- общий объем выполненной работы, при этом должны быть применены единицы измерения для четкой квалиметрии результатов и последующего выставления оценки за занятие;
- отдельно объем работы, который должен повлиять на показатели работы другой группы, например «злоумышленник - администратор», или «администратор -руководитель».

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1. Перечень контрольных вопросов

1. Структура политики информационной безопасности и процесс ее разработки
2. Характеристика различных уровней политики ИБ
3. Уровни организационной работы в сфере информационной безопасности.
4. Стандарты управления информационной безопасностью.
5. Основные направления управленческой (организационной) работы в сфере ИБ на уровне отдельного предприятия.
6. Департамент информационной безопасности. Управление персоналом
7. Этапы разработки и внедрения системы управления ИБ
8. Содержание этапов разработки и внедрения системы управления ИБ
9. Понятие аудита безопасности
10. Методы анализа данных при аудите ИБ

Для проверки сформированности компетенции ПК-2. Способен осуществлять сбор, анализ и систематизацию научно-технической информации по вопросам обеспечения информационной безопасности объектов информатизации

ИПК-2.1. Проводит анализ безопасности объектов информатизации

Блок А. Задания репродуктивного уровня («знать»)

А.1 Тестовые задания по дисциплине

1. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
б) Когда необходимые защитные меры слишком сложны
в) Когда риски не могут быть приняты во внимание по политическим соображениям
г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

2. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) Анализ рисков
б) Выявление уязвимостей и угроз, являющихся причиной риска
в) Анализ затрат / выгоды

3.Что не относится к способам обработки рисков?

а) Уклонение от рисков
б) Принятие рисков
в) Снижение рисков
г) Замена рисков
д) Передача рисков

4. Укажите последовательность этапов ***оценки информационных рисков***:

1	оценивание эффективности средств обеспечения информационной безопасности
3	оценивание возможных угроз
2	оценивание существующих уязвимостей
4	идентификация и количественная оценка информационных ресурсов предприятий, значимых для бизнеса

5. Дополните перечень видов активов:

а) информационные ресурсы
б) программное обеспечение
в) материальные активы
г) сервисы
д) _____
е) _____

6. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) Сотрудники
б) Хакеры
в) Контрагенты (лица, работающие по договору)
г) Атакующие.

7. Что самое главное должно продумать руководство при классификации данных?

а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

б) Оценить уровень риска и отменить контрмеры
в) Необходимый уровень доступности, целостности и конфиденциальности
г) Управление доступом, которое должно защищать данные

8. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) Владельцы данных
б) Пользователи
в) Администраторы
г) Руководство

А2. Вопросы для устного опроса

1. Системный подход к управлению рисками.
2. Составляющие процесса управления рисками ИБ.
3. Этапы оценки рисков ИБ.
4. Понятие актива. Типы активов. Инвентаризация активов. Источники информации об активах организации.
5. Определение угроз ИБ, уязвимостей и последствий на этапе инвентаризации активов. Подходы к оценке рисков ИБ.
6. Планирование мер по обработке выявленных рисков ИБ.
7. Обеспечение управления рисками ИБ. Управление инцидентами ИБ

Блок В. Задания реконструктивного уровня («уметь»)

В1. Практическая работа

Рассчитать риск информационной безопасности сервера на основе модели угроз и уязвимостей с учетом следующих исходных данных.

1. Угрозы и уязвимости

Ресурс	Угрозы	Уязвимости
Сервер (критичность ресурса 100 у.е.)	Угроза 1 Неавторизованное проникновение нарушителя внутрь охраняемого периметра (одного из периметров)	Уязвимость 1 Отсутствие регламента доступа в помещения с ресурсами, содержащими ценную информацию
		Уязвимость 2 Отсутствие системы наблюдения (видеонаблюдение, сенсоры и т.д.) за объектом (или существующая система наблюдения охватывает не все

		важные объекты)
	Угроза 2 Неавторизованная модификация информации в системе электронной почты, хранящейся на ресурсе	Уязвимость 1 Отсутствие авторизации для внесения изменений в систему электронной Почты
		Уязвимость 2 Отсутствие регламента работы с системой криптографической защиты электронной корреспонденции
	Угроза 3 Разглашение конфиденциальной информации сотрудниками компании	Уязвимость 1 Отсутствие соглашений о конфиденциальности
		Уязвимость 2 Распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими доверенными сотрудниками

Вероятность реализации

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)	Критичность реализации угрозы через уязвимость (%). ER
Угроза 1/Уязвимость 1	50	60
Угроза 1/Уязвимость 2	20	60
Угроза 2/Уязвимость 1	60	40
Угроза 2/Уязвимость 2	10	40
Угроза 3/Уязвимость 1	10	80
Угроза 3/Уязвимость 2	80	80

В2. Тематика рефератов

1. Организационно-правовое обеспечение информационной безопасности бизнеса.
2. Выявление рисков нарушения информационной безопасности предприятия.
3. Международно-правовые аспекты информационной безопасности.
4. Классификация возможных угроз безопасности.
5. Организация информационной безопасности в коммерческом секторе. Организация системы безопасности корпоративных информационных систем.
6. Инженерно-техническая безопасность предприятия.
7. Информационная собственность и ее защита.

8. Информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения и механизмов информационной безопасности.
9. Существующие способы устранения угроз.

В3. Тематика презентаций

1. Организационно-правовое обеспечение информационной безопасности бизнеса.
2. Выявление рисков нарушения информационной безопасности предприятия.
3. Международно-правовые аспекты информационной безопасности.
4. Классификация возможных угроз безопасности.
5. Организация информационной безопасности в коммерческом секторе. Организация системы безопасности корпоративных информационных систем.
6. Инженерно-техническая безопасность предприятия.
7. Информационная собственность и ее защита.
8. Информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения и механизмов информационной безопасности.
9. Существующие способы устранения угроз.

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С.1. Кейсы

Кейс «Расчет рисков информационной безопасности»

Описание ситуации:

Например, информационная система Компании состоит из двух ресурсов: сервера и рабочей станции, которые находятся в одной сетевой группе, т.е. физически связанны между собой.

На сервере хранятся виды информации: бухгалтерский отчет и база клиентов Компании.

На рабочей станции расположена база данных наименований товаров Компании с описанием. К серверу локальный доступ имеет группа пользователей (к первой информации – бухгалтерский отчет):

- главный бухгалтер. К серверу удаленный доступ имеют группы пользователей (ко второй информации – база клиентов Компании):
- бухгалтер (с рабочей станции);
- финансовый директор (через глобальную сеть Интернет).

К рабочей станции локальный доступ имеет группа пользователей (к базе данных наименований товаров Компании с описанием):

– бухгалтер.

По правилам работы модели бухгалтер при удаленном доступе к серверу является группой обычных пользователей, а финансовый директор – группой авторизованных пользователей. Причем, бухгалтер имеет удаленный доступ к серверу через коммутатор.

Задание: Рассчитать риски информационной безопасности на основе модели информационных потоков.

С2. Проектная работа.

Практическая работа (проект)

1. Разработка модели угроз ИБ конкретного объекта.
2. Разработка модели нарушителя ИБ конкретного объекта.
3. Разработка политики ИБ конкретного объекта.
4. Оценка рисков ИБ конкретного объекта.
5. Проектирование отдельного процесса СУИБ конкретного объекта.
6. Разработка структуры СУИБ конкретного объекта.
7. Разработка плана проведения аудита ИБ конкретного объекта.

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень контрольных вопросов

1. Методы оценивания информационных рисков
2. Управление информационными рисками
3. Этапы процесса управления рисками
4. Метод оценки рисков, основанный на построении модели угроз и уязвимостей
5. Метод оценки рисков, основанный на построении модели информационных потоков.

РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Балльно-рейтинговая система является базовой системой оценивания сформированности компетенций обучающихся очной формы обучения.

Итоговая оценка сформированности компетенции(й) обучающихся в рамках балльно-рейтинговой системы осуществляется в ходе текущего контроля успеваемости, промежуточной аттестации и определяется как сумма баллов, полученных обучающимися в результате прохождения всех форм контроля.

Оценка сформированности компетенции(й) по дисциплине складывается из двух составляющих:

✓ первая составляющая – оценка преподавателем сформированности компетенции(й) в течение семестра в ходе текущего контроля успеваемости (максимум 100 баллов). Структура первой составляющей определяется технологической картой дисциплины, которая в начале семестра доводится до сведения обучающихся;

✓ вторая составляющая – оценка сформированности компетенции(й) обучающихся на экзамене (максимум – 30 баллов).

Для студентов очно-заочной формы обучения применятся 4-балльная и бинарная шкалы оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся.

уровни освоения компетенций	продвинутый уровень	базовый уровень	пороговый уровень	допороговый уровень
100 – балльная шкала	85 и ≥	70 – 84	51 – 69	0 – 50
4 – балльная шкала	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»

Шкала оценок при текущем контроле успеваемости по различным показателям

Показатели оценивания сформированности компетенций	***Баллы***	***Оценка***
Выполнение практических заданий	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Решение кейсов	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Устный опрос	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Подготовка реферата	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Подготовка презентации	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение проекта	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение письменной работы	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Участие в деловой игре	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по текущему контролю успеваемости

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-50	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины
51-69	«удовлетворительно»	Пороговый уровень	Не менее 50% заданий, подлежащих текущему контролю успеваемости, выполнены без существенных ошибок
70-84	«хорошо»	Базовый уровень	Обучающимся выполнено не менее 75% заданий, подлежащих текущему

			контролю успеваемости, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала и применения его при решении практических заданий; задания выполнены без ошибок
85-100	«отлично»	Продвинутый уровень	100% заданий, подлежащих текущему контролю успеваемости, выполнены самостоятельно и в требуемом объеме; обучающийся проявляет умение обобщать, систематизировать материал и применять его при решении практических заданий; задания выполнены с подробными пояснениями и аргументированными выводами

Шкала оценок по промежуточной аттестации

Наименование формы промежуточной аттестации	***Баллы***	***Оценка***
Экзамен	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-9	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы
10-16	«удовлетворительно»	Пороговый уровень	Обучающийся дал неполные ответы на вопросы, с недостаточной

			аргументацией, практические задания выполнены не полностью, компетенции, осваиваемые в процессе изучения дисциплины сформированы не в полном объеме.
17-23	«хорошо»	Базовый уровень	Обучающийся в целом приобрел знания и умения в рамках осваиваемых в процессе обучения по дисциплине компетенций; обучающийся ответил на все вопросы, точно дал определения и понятия, но затрудняется подтвердить теоретические положения практическими примерами; обучающийся показал хорошие знания по предмету, владение навыками систематизации материала и полностью выполнил практические задания
25-30	«отлично»	Продвинутый уровень	Обучающийся приобрел знания, умения и навыки в полном объеме, закрепленном рабочей программой дисциплины; терминологический аппарат использован правильно; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать материал и выполняет практические задания с подробными пояснениями и аргументированными выводами

РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций

Методика оценивания ответов на устные вопросы

Баллы	***Оценка***	***Показатели***	***Критерии***
5	«отлично»	1. Полнота данных ответов; 2. Правильность ответов на вопросы.	Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, привести необходимые примеры. Изложение

			материала последовательно и правильно.
3-4	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
1-2	«удовлетворительно»		Студент обнаруживает знание и понимание основных положений данного задания, но: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки.
0	«неудовлетвори-тельно»		Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

Тестирование проводится с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного университета народного хозяйства.

На тестирование отводится 45 минут. Каждый вариант тестовых заданий включает 30 вопросов.

Методика оценивания выполнения тестов

Баллы	Оценка	Показатели	Критерии
25-30	«отлично»	1. Полнота выполнения тестовых заданий; 2. Своевременность выполнения; 3. Правильность ответов на вопросы.	Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос
19-24	«хорошо»		Выполнено более 70 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос; однако были допущены неточности в определении понятий, терминов и др.
15-18	«удовлетворительно»		Выполнено более 54 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со

			стилистическими и орфографическими ошибками.
0-14	«неудовле твори-тельно»		Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

Тема реферата выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На написание реферата отводится одна неделя. Реферат оформляется согласно действующим в Дагестанском государственном университете народного хозяйства требованиям к оформлению письменных работ. Объем представленного реферата должен быть не менее 10 страниц машинописного текста без учета титульного листа.

Публичная защита реферата проводится в присутствии остальных студентов, защищающих рефераты. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель реферата, а также цельно сформулировать базовую идею, отраженную в реферате.

Методика оценивания выполнения рефератов

Баллы	***Оценка***	***Показатели***	***Критерии***
5	«отлично»	1. Полнота выполнения рефератов; 2. Своевременность выполнения; 3. Четкость изложения идеи реферата во время защиты.	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, четкое и последовательное выступление во время защиты.
3-4	«хорошо»		Основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; выступление во время защиты требует дополнительных вопросов.
1-2	«удовлетв орительно		Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены

	»		фактические ошибки в содержании реферата или при ответе на дополнительные вопросы во время выступления.
0	«неудовле твори-тельно»		Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы, не проведена защита реферата.

Тема презентации выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На подготовку презентации отводится одна неделя.

Публичная презентация проводится в присутствии остальных студентов. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель презентации, а также цельно сформулировать базовую идею.

Методика оценивания выполнения презентаций

Баллы	***Оценка***	***Показатели***	***Критерии***
5	«отлично»	4. Полнота выполнения; 5. Своевременность выполнения; 6. Четкость изложения идеи презентации во время защиты.	Выполнены все требования к подготовке презентации: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, четкое и последовательное выступление во время демонстрации.
3-4	«хорошо»		Основные требования к подготовке презентации выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем презентации; имеются упущения в оформлении; выступление во время демонстрации требует дополнительных вопросов.
1-2	«удовлетв орительно »		Имеются существенные отступления от требований к презентации. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании презентации или при ответе на дополнительные вопросы во время выступления.

0	«неудовле твори-тельно»		Тема презентации не раскрыта, обнаруживается существенное непонимание проблемы, не проведена демонстрация презентации.

Практические задания выполняются непосредственно во время занятий семинарского типа (одно задание на одну пару согласно текущей тематике занятия). Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности представленного решения. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения задания, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания выполнения практических заданий

Баллы	***Оценка***	***Показатели***	***Критерии***
5	«отлично»	1. Полнота выполнения практического задания; 2. Своевременность выполнения задания; 3. Самостоятельность решения.	Основные требования к выполнению задания выполнены. Продемонстрировано умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели
3-4	«хорошо»		Основные требования к выполнению задания реализованы, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений
1-2	«удовлетв орительно »		Имеются существенные отступления от выполнения работы. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат
0	«неудовле твори-тельно»		Задача выполнения работы не раскрыта, обнаруживается существенное непонимание проблемы

Ответы на ситуационные задачи (кейс-здачи) оформляются студентом в письменном виде и сдаются преподавателю в электронной форме с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного университета народного хозяйства.

На решение каждой кейс-задачи отводится 45 минут. Представленный ответ должен отражать однозначную позицию по поставленной задаче.

Методика оценивания решения ситуационных задач (кейс-задач)

Баллы	***Оценка***	***Показатели***	***Критерии***
5	«отлично»	1. Полнота решения задач; 2. Своевременность выполнения; 3. Правильность ответов на вопросы.	Основные требования к решению задач выполнены. Продемонстрированы умение анализировать ситуацию и находить оптимальное количество решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для уточнения ситуации, навыки четкого и точного изложения собственной точки зрения в устной и письменной форме, убедительного отстаивания своей точки зрения.
3-4	«хорошо»		Основные требования к решению задач выполнены, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений.
1-2	«удовлетворительно»		Имеются существенные отступления от решения задач. В частности отсутствуют навыки и умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат.
0	«неудовлетвори-тельно»		Ситуационная задача не решена, обнаруживается существенное непонимание проблемы.

Основная цель проекта – провести имитацию разработки организационно-распорядительной документации организации. В рамках группового проекта необходимо подготовить политику безопасности и документы 2-3 уровня политики выбранной организации. Документы, которые должны быть по внешнему виду (оформлению, содержанию) аналогичны реальным документам.

Методика оценивания выполнения проекта

Баллы	***Оценка***	***Показатели***	***Критерии***
9-10	«отлично»	1. Полнота выполнения задания; 2. Своевременность выполнения задания; 3. Полнота и качество	Документы, характеризующие политику безопасности организации, приведены в полном объеме и аналогичны по оформлению и содержанию их реальным аналогам.
8-7	«хорошо»		Документы, характеризующие политику безопасности организации,

		предоставленных материалов	приведены в полном объеме, но содержат незначительные ошибки.
5-6	«удовлетворительно»		Документы, характеризующие политику безопасности организации, приведены не в полном объеме, наличествующие содержат незначительные ошибки в заполнении.
0-4	«неудовлетвори-тельно»		Документы, характеризующие политику безопасности организации, приведены не в полном объеме, наличествующие содержат грубые ошибки при заполнении или не соответствуют реальным документам.

Методика оценивания участников деловой игры

Баллы	***Оценка***	***Показатели***	***Критерии***
5	«отлично»	1. Полнота достижения цели; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. и т.д.	Основные требования к решению учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации выполнены. Продемонстрировано умение анализировать и решать типичные профессиональные задачи
3-4	«хорошо»		Основные требования к решению учебных и профессионально-ориентированных задач деловой игры выполнены, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений
1-2	«удовлетворительно»		Имеются существенные отступления от достижения поставленной цели деловой игры. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат

0	«неудовлетвор ительно»		Задача деловой игры не раскрыта, обнаруживается существенное непонимание проблемы

Методика оценивания письменных работ

Баллы	***Оценка***	***Показатели***	***Критерии***
25-30	«отлично»	3. Полнота данных ответов; 4. Правильность ответов на вопросы.	Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, привести необходимые примеры. Изложение материала последовательно и правильно.
19-24	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
15-18	«удовлетв орительно »		Студент обнаруживает знание и понимание основных положений данного задания, но: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки.
0-14	«неудовле твори-тельно»		Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

Процедура промежуточной аттестации проходит в соответствии с Положением о промежуточной аттестации знаний студентов и учащихся ДГУНХ.

Аттестационные испытания проводятся преподавателем, ведущим лекционные занятия по данной дисциплине, или преподавателями, ведущими практические и лабораторные занятия (кроме устного экзамена). Присутствие посторонних лиц в ходе проведения аттестационных испытаний без разрешения ректора или проректора по учебной работе не допускается (за исключением работников университета, выполняющих контролирующие функции в соответствии со своими должностными обязанностями). В случае отсутствия ведущего преподавателя аттестационные испытания проводятся преподавателем, назначенным письменным распоряжением по кафедре (структурному подразделению).

Инвалиды и лица с ограниченными возможностями здоровья, имеющие нарушения опорно-двигательного аппарата, допускаются на аттестационные испытания в сопровождении ассистентов-сопровождающих.

Во время аттестационных испытаний обучающиеся могут пользоваться программой дисциплины, а также с разрешения преподавателя справочной и нормативной литературой, непрограммируемыми калькуляторами.

Лист актуализации оценочных материалов по дисциплине «Анализ рисков и аудит информационной безопасности автоматизированных систем»

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____