ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утверждены решением
Ученого совета ДГУНХ,
протокол № 9
от 24 марта 2025 г

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПО ДИСЦИПЛИНЕ «ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ»

НАПРАВЛЕНИЕ ПОДГОТОВКИ – 10.03.01
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПРОФИЛЬ
«БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Уровень высшего образования - бакалавриат

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00C5A9FA0FAD6D6153888A98846B419FD3
Владелец: Бучаев Ахмед Гамидович
Действителен: с 11.07.2024 до 04.10.2025

Махачкала – 2025

УДК 681.518(075.8)
ББК 32.81.73

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

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент кафедры «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 «Основы управления информационной безопасностью в автоматизированных системах» разработаны в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, в соответствии с приказом Министерства науки и высшего образования Российской Федерации от 6.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Оценочные материалы по дисциплине «Основы управления информационной безопасностью в автоматизированных системах» размещены на официальном сайте www.dgunh.ru

Гасанова З.А. Оценочные материалы по дисциплине «Основы управления информационной безопасностью в автоматизированных системах» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2025 г. – 39 с.

Рекомендованы к утверждению Учебно-методическим советом ДГУНХ 10 марта 2025 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» 24 февраля 2025 г., протокол № 7.

СОДЕРЖАНИЕ

Назначение оценочных материалов……..4

РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины ..…….……5

1.1 Перечень формируемых компетенций……5

1.2 Перечень компетенций с указанием видов оценочных средств…….5

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине…….14

РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания……..28

РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций…….31

Лист актуализации оценочных материалов по дисциплине……..39

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 «Основы управления информационной безопасностью в автоматизированных системах» на соответствие их учебных достижений поэтапным требованиям образовательной программы высшего образования 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»

Оценочные материалы по дисциплине «Основы управления информационной безопасностью в автоматизированных системах» 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-1	Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей
ПК-4	Способен планировать и организовывать комплекс мероприятий и разрабатывать организационно-распорядительную документацию по защите информации

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-1. Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционн	ИПК-1.5. Управляет защитой информации в автоматизированных системах	**Знать:** - методы администрирования подсистем обеспечения безопасности средств защиты информации; - методы анализа защищенности автоматизированных систем.	Пороговый уровень	Обучающийся слабо (частично) знает методы администрирования подсистем обеспечения безопасности средств защиты информации, методы анализа защищенности автоматизированных систем.	**Блок А –** задания репродуктивного уровня – вопросы для устного опроса
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает методы	

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*
ых систем, систем управления базами данных и компьютерных сетей				администрирования подсистем обеспечения безопасности средств защиты информации, методы анализа защищенности автоматизированных систем.	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает методы администрирования подсистем обеспечения безопасности средств защиты информации, методы анализа защищенности автоматизированных систем.	
		Уметь: - проводить администрирование подсистем обеспечения безопасности средств защиты информации; - проводить анализ защищенности отельных подсистем средств защиты информации.	Пороговый уровень	Обучающийся слабо (частично) умеет проводить администрирование подсистем обеспечения безопасности средств защиты информации, проводить анализ защищенности отельных подсистем средств защиты информации.	**Блок В** – задания реконструктивного уровня - тематика рефератов; - тематика презентаций;
			Базовый уровень	Обучающийся с незначительными затруднениями умеет проводить администрирование	

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*
				подсистем обеспечения безопасности средств защиты информации, проводить анализ защищенности отельных подсистем средств защиты информации.	
			Продвинутый уровень	Обучающийся умеет проводить администрирование подсистем обеспечения безопасности средств защиты информации, проводить анализ защищенности отельных подсистем 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 - деловая игра. - лабораторные работы.
			Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками тестирования подсистем обеспечения безопасности средств защиты информации.	
			Продвинутый уровень	Обучающийся свободно владеет	

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*
				навыками тестирования подсистем обеспечения безопасности средств защиты информации.	
ПК-4. Способен планировать и организовывать комплекс мероприятий и разрабатывать организационно-распорядительную документацию по защите информации	ИПК-4.1. Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах	**Знать:** - регламенты устранения и учёта выявленных инцидентов; - регламент информирования персонала автоматизированной системы о выявленных инцидентах.	Пороговый уровень	- Обучающийся слабо (частично) знает регламенты устранения и учёта выявленных инцидентов, регламент информирования персонала автоматизированной системы о выявленных инцидентах.	**Блок А –** задания репродуктивного уровня - тестовые задания; – вопросы для устного опроса
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает регламенты устранения и учёта выявленных инцидентов, регламент информирования персонала автоматизированной системы о выявленных инцидентах.	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает регламенты устранения и учёта	

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*
				выявленных инцидентов, регламент информирования персонала автоматизированной системы о выявленных инцидентах.	
		Уметь: - разрабатывать документы, регламентирующие процессы управления информационной безопасностью в автоматизированных системах.	Пороговый уровень	Обучающийся слабо (частично) умеет разрабатывать документы, регламентирующие процессы управления информационной безопасностью в автоматизированных системах.	**Блок В** – задания реконструктивного уровня – тематика рефератов; - тематика презентаций.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет разрабатывать документы, регламентирующие процессы управления информационной безопасностью в автоматизированных системах.	
			Продвинутый уровень	Обучающийся умеет разрабатывать документы, регламентирующие процессы управления информационной безопасностью в автоматизированных системах.	

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*
		Владеть: - навыками разработки организационно-распорядительных документов по защите информации в автоматизированных системах.	Пороговый уровень	Обучающийся слабо (частично) владеет навыками разработки организационно-распорядительных документов по защите информации в автоматизированных системах.	**Блок С** – задания практико-ориентированного уровня – проектная работа.
			Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками разработки организационно-распорядительных документов по защите информации в автоматизированных системах.	
			Продвинутый уровень	Обучающийся свободно владеет навыками разработки организационно-распорядительных документов по защите информации в автоматизированных системах.	
	ИПК-4.2. Внедряет организационные меры по защите информации в автоматизиро	**Знать:** - процессы, процедуры, методы управления информационной безопасность	Пороговый уровень	Обучающийся слабо (частично) знает процессы, процедуры, методы управления информационной безопасностью защищённых	**Блок А –** задания репродуктивного уровня – тестовые задания; – вопросы для

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*
	ванных системах	ю защищённых автоматизированных систем организаций.		автоматизированных систем организаций.	устного опроса
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает процессы, процедуры, методы управления информационной безопасностью защищённых автоматизированных систем организаций.	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает процессы, процедуры, методы управления информационной безопасностью защищённых автоматизированных систем организаций.	
		Уметь: - определять и обосновывать активы, ресурсы, роли, деятельности для процессов и процедур управления информационной	Пороговый уровень	Обучающийся слабо (частично) умеет определять и обосновывать активы, ресурсы, роли, деятельности для процессов и процедур управления информационной безопасности защищённых автоматизированных систем управления и организаций.	**Блок В** – задания реконструктивного уровня – тематика рефератов; - тематика презентаций; - практическая работа.

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 управления и организаций.	Базовый уровень	Обучающийся с незначительными затруднениями умеет определять и обосновывать активы, ресурсы, роли, деятельности для процессов и процедур управления информационной безопасности защищённых автоматизированных систем управления и организаций.	
			Продвинутый уровень	Обучающийся умеет определять и обосновывать активы, ресурсы, роли, деятельности для процессов и процедур управления информационной безопасности защищённых автоматизированных систем управления и организаций.	
		Владеть: - навыками определения правил и процедур выявления инцидентов и процедур реагирования на инциденты.	Пороговый уровень	Обучающийся слабо (частично) владеет навыками определения правил и процедур выявления инцидентов и процедур реагирования на инциденты.	**Блок С** – задания практико-ориентированного уровня - практическая работа.
			Базовый уровень	Обучающийся с небольшими	

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***
				затруднениями владеет навыками определения правил и процедур выявления инцидентов и процедур реагирования на инциденты.	
			Продвинутый уровень	Обучающийся свободно владеет навыками определения правил и процедур выявления инцидентов и процедур реагирования на инциденты.	

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

Для проверки сформированности компетенции ПК-1. Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей
ИПК-1.5. Управляет защитой информации в автоматизированных системах

Блок А. Задания репродуктивного уровня («знать»)

А1. Вопросы для устного опроса

1. Автоматизированные рабочие места, пользователи и эксплуатационный персонал.
2. Указ Президента РФ от 06.03.1997 N 188 «Об утверждении перечня сведений конфиденциального характера и организации работы по защите конфиденциальной информации в федеральной службе по надзору в сфере образования и науки и подведомственных ей государственных учреждениях.
3. Понятие угрозы, угрозы безопасности информации в компьютерных системах.
4. Классификационные схемы (каталогизация) угроз. Каталог угроз по BSI.
5. Примеры угроз защищаемым активам в продуктах и системах ИТ (по РД Гостехкомиссии «Безопасность ИТ. Руководство по разработке профилей защиты и заданий по безопасности»). Идентификация и спецификация (описание) угроз – выявление угрозы определенного типа и присвоение ей уникального идентификатора.
6. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации от 30 марта 1992 г. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов

1. Принципы и средства построения систем информационной безопасности
2. Этапы создания систем защиты информации
3. Моделирование системы защиты информации
4. Системный подход к защите информации и показатели безопасности информации

5. Требования к структуре системы защиты информации
6. Мероприятия, способы и средства по обеспечению защиты информации на объекте
7. Комплекс мероприятий по обеспечению информационной безопасности
8. Технические средства защиты информации
9. Категории средств защиты информационно-программного обеспечения

В2. Тематика презентаций

1. Принципы и средства построения систем информационной безопасности
2. Этапы создания систем защиты информации
3. Моделирование системы защиты информации
4. Системный подход к защите информации и показатели безопасности информации
5. Требования к структуре системы защиты информации
6. Мероприятия, способы и средства по обеспечению защиты информации на объекте
7. Комплекс мероприятий по обеспечению информационной безопасности
8. Технические средства защиты информации
9. Категории средств защиты информационно-программного обеспечения

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

С1. 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.

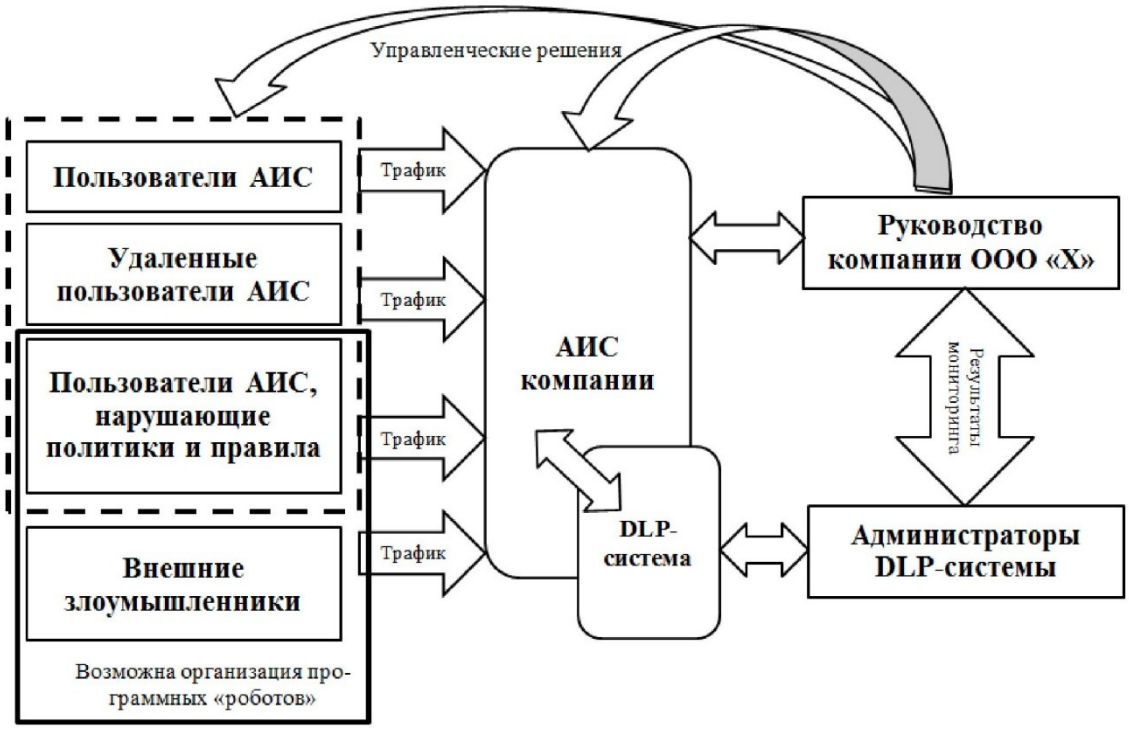

Рисунок 2. Распределение ролей участников игры и организация взаимодействия между ними

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».

С2. Лабораторные работы.

Лабораторная работа №1. Определение защищенной информационной системы.
Лабораторная работа №2. Методология анализа защищенности информационной системы.
Лабораторная работа №3. Требования к архитектуре информационной системы для обеспечения безопасности ее функционирования
Лабораторная работа № 4. Этапы построения системы безопасности ИС.
Лабораторная работа №5. Профиль защиты.
Лабораторная работа № 6. Анализ защищенности автоматизированной системы.

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1. Перечень контрольных вопросов

Для проверки сформированности компетенции ПК-4. Способен планировать и организовывать комплекс мероприятий и разрабатывать организационно-распорядительную документацию по защите информации
ИПК-4.1. Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах

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

А2. Вопросы для устного опроса

1. Структура и содержание Политики безопасности автоматизированных систем.
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.

Блок В. Задания реконструктивного уровня («уметь»)

В1. 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

В2. 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

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

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

Для проверки сформированности компетенции ПК-4. Способен планировать и организовывать комплекс мероприятий и разрабатывать организационно-распорядительную документацию по защите информации

ИПК-4.2. Внедряет организационные меры по защите информации в автоматизированных системах

Блок А. Задания репродуктивного уровня («знать»)

А.1 Тестовые задания по дисциплине.

1. ***Событие ИБ*** *– это…*
   а) идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики ИБ или аварию защитных мер (средств), а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью
   б) идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики ИБ или аварию защитных мер (средств)
   в) нарушение политики ИБ или авария защитных мер (средств) системы
2. ***Инцидент ИБ*** *- это…*
   а) одно или серия нежелательных событий ИБ, которые имеют значительную вероятность компрометации бизнес-операций (бизнес-функций) и угрожают информационной безопасности
   б) события ИБ, которые угрожают информационной безопасности
   в) нежелательные события ИБ, которые компрометируют бизнес-операции

А2. Вопросы для устного опроса

1. Обнаружение событий ИБ, которые могут быть причиной инцидента ИБ с помощью:
   1) программных средств
   2) сотрудников.
2. Анализ инцидента ИБ. Первичная оценка инцидента ИБ. Вторичная оценка инцидента ИБ.
3. Выработка стратегии сдерживания инцидентов ИБ. Выработка стратегии по устранению инцидентов ИБ.
4. Формирование итоговой отчётности об инциденте ИБ.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Практические задания

1. Привести пример формы сообщения «Отчет о событии ИБ» сотрудника, обнаружившего нештатную ситуацию, имеющую отношение к ИБ
2. Привести пример формы сообщения «Отчет об инциденте ИБ» сотрудника ГРИИБ, проводившего первичную оценку событий ИБ
3. Привести пример матрицы для определения значимости инцидентов

неавторизованного доступа
4. Определить предвестники и указатели инцидентов неавторизованного доступа
5. Определить меры по сдерживанию, устранению инцидентов неавторизованного доступа и восстановлению после них
6. Привести пример матрицы для определения значимости инцидентов отказа в обслуживании
7. Определить предвестники и указатели инцидентов отказа в обслуживании
8. Определить меры по сдерживанию, устранению инцидентов отказа в обслуживании и восстановлению после них
9. Привести пример матрицы для определения значимости инцидентов сбора информации
10. Определить предвестники и указатели инцидентов сбора информации
11. Определить меры по сдерживанию, устранению инцидентов сбора информации и восстановлению после них
12. Привести пример матрицы для определения значимости инцидентов внедрения вредоносного кода
13. Определить предвестники и указатели инцидентов внедрения вредоносного кода
14. Определить меры по сдерживанию, устранению инцидентов внедрения вредоносного кода и восстановлению после них
15. Привести пример матрицы для определения значимости инцидентов несоответствующего использования
16. Определить предвестники и указатели инцидентов несоответствующего использования. Определить меры по сдерживанию, устранению инцидентов несоответствующего использования и восстановлению после них

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

С.1. Практическая работа

1. Построить возможные сценарии инцидента неавторизованного доступа
2. Построить возможные сценарии инцидента отказа в обслуживании
3. Построить возможные сценарии инцидента внедрения вредоносного кода
4. Построить возможные сценарии инцидента сбора информации
5. Построить возможные сценарии инцидента несоответствующего использования

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1. Перечень контрольных вопросов

1. Формирование политики управления инцидентами ИБ. Основное содержание политики управления инцидентами ИБ
2. Создание группы реагирования на инциденты ИБ. Цель создания. Роли группы реагирования на инциденты ИБ
3. Подготовка к обработке инцидентов ИБ. Классификация инцидентов ИБ по значимости
4. Обеспечение осведомленности и обучение управлению инцидентами. Цель осведомления об управлении инцидентами ИБ. Цель обучения управлению инцидентами ИБ
5. Тестирование системы управления инцидентами ИБ
6. Первичная оценка событий ИБ. Цель проведения первичной оценки. Последовательность действий при проведении первичной оценки
7. Вторичная оценка инцидента ИБ. Цель проведения вторичной оценки. Последовательность действий при проведении вторичной оценки
8. Сдерживание, устранение инцидента ИБ и восстановление после него
9. Формирование и хранение свидетельств инцидентов ИБ
10. Определение инцидента неавторизованного доступа. Цели инцидента неавторизованного доступа
11. Определение инцидента отказа в обслуживании. Цели инцидента отказа в обслуживании. Примеры инцидентов отказа в обслуживании
12. Определение инцидента сбора информации. Цели инцидента сбора информации
13. Определение инцидента внедрения вредоносного кода. Средства реализации инцидента внедрения вредоносного кода. Цели инцидента
14. Определение инцидента несоответствующего использования. Примеры инцидентов несоответствующего использования
15. Стратегии управления непрерывностью функционирования АС для помещений и технологий
16. Стратегии управления непрерывностью функционирования АС для данных. Стратегии управления непрерывностью функционирования АС для поставщиков
17. Стратегии управления непрерывностью функционирования АС для компьютеров
18. Стратегии управления непрерывностью функционирования АС для серверов
19. Стратегии управления непрерывностью функционирования АС для локальной сети

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 – 20 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
Бинарная шкала	Зачтено			Не зачтено

Шкала оценок при текущем контроле успеваемости по различным показателям

Показатели оценивания сформированности компетенций	***Баллы***	***Оценка***
Выполнение практических заданий	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 лабораторной работы	0-15	«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	Обучающимся выполнено не менее

		уровень	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***
Зачет	0-20	«не зачтено» «зачтено»

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-9	«не зачтено»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы
10-14	«зачтено»	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.
15-17	«зачтено»	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
18-20	«зачтено»	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	«неудовлетворительно»		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	«удовлетворительно»		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	«неудовлетвори-		Тема презентации не раскрыта, обнаруживается существенное непонимание

	тельно»		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	«удовлетворительно»		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	«неудовлетвори-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 выполнения проекта

Баллы	*Оценка*	*Показатели*	*Критерии*
9-10	«отлично»	1. Полнота выполнения задания; 2. Своевременность выполнения задания; 3. Полнота и качество предоставленных материалов	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, 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

Лабораторные работы выполняются в специализированной аудитории во время лабораторных занятий. Предусмотрено выполнение одной лабораторной работы в течение одного занятия согласно текущей тематике. Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности полученного результата. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения шагов лабораторной работы, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания выполнения *лабораторных работ*

Баллы	***Оценка***	***Показатели***	***Критерии***
18-20	«отлично»	4. Полнота выполнения задания лабораторной работы; 5. Своевременность выполнения задания лабораторной работы; 6. Самостоятельность решения.	Основные требования к выполнению задания лабораторной работы 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
14-17	«хорошо»		Основные требования к выполнению задания лабораторной работы 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
11-13	«удовлетв орительно »		Имеются существенные отступления от выполнения лабораторной работы. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат
0-10	«неудовле твори-		Шаги выполнения лабораторной работы не выполнены, обнаруживается существенное

	тельно»		непонимание проблемы.

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 «Основы управления информационной безопасностью»

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 _____