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 «КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ»

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 004.056
ББК 32.973.202

Составитель – Меджидов Заур Уруджалиевич, кандидат экономических наук, доцент кафедры «Информационные технологии и информационная безопасность».

Внутренний рецензент – Раджабов Карахан Якубович, кандидат экономических наук, доцент, доцент кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдуллаев Ших-Саид Омаржанович, доктор технических наук, главный научный сотрудник Отдела математики и информатики Дагестанского научного центра Российской академии наук.

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

Оценочные материалы по дисциплине «Комплексная защита объектов информатизации» 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 «Комплексная защита объектов информатизации» размещены на официальном сайте www.dgunh.ru

Меджидов З.У. Оценочные материалы по дисциплине «Комплексная защита объектов информатизации» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2025 г. – 56 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……20

РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания……..44

РАЗДЕЛ 4.Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций…….47

Лист актуализации оценочных материалов по дисциплине……..56

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 «Комплексная защита объектов информатизации» на соответствие их учебных достижений поэтапным требованиям образовательной программы высшего образования 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»

Оценочные материалы по дисциплине «Комплексная защита объектов информатизации» 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
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений
ОПК-4.4	Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем

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***
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами	ОПК-6.2. Подготавливает объект информатизации для прохождения аттестации на соответствие требованиям государственных и ведомственных нормативных документов	**Знать:** – виды аттестаций объектов информатизаций; – принципы выстраивания комплексной защиты информации в соответствии с нормативно-методическими документами ФСБ России, ФСТЭК России.	Пороговый уровень	Обучающийся слабо (частично) знает виды аттестаций объектов информатизаций, принципы выстраивания комплексной защиты информации в соответствии с нормативно-методическими документами ФСБ России, ФСТЭК	**Блок А –** задания репродуктивного уровня – тестовые задания; – контрольные вопросы

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***
Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю				России	
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает виды аттестаций объектов информатизаций, принципы выстраивания комплексной защиты информации в соответствии с нормативно-методическими документами ФСБ России, ФСТЭК России	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает виды аттестаций объектов информатизаций, принципы выстраивания комплексной защиты информации в соответствии с	

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*
				нормативно-методическими документами ФСБ России, ФСТЭК России	
		<u>Уметь</u>: - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации ограниченного доступа; – применять отечественные и зарубежные стандарты в области информационной безопасности для оценки защищенности объектов информатизации; – пользоваться нормативными документами по защите информации	Пороговый уровень	Обучающийся слабо (частично) умеет определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации ограниченного доступа, применять отечественные и зарубежные стандарты в области информационной безопасности для оценки защищенности объектов информатизации, пользоваться нормативными документами	**Блок В** – задания реконструктивного уровня – лабораторная работа; – темы рефератов; - темы презентаций

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*
				по защите информации	
			Базовый уровень	Обучающийся с незначительными затруднениями умеет определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации ограниченного доступа, применять отечественные и зарубежные стандарты в области информационной безопасности для оценки защищенности объектов информатизации, пользоваться нормативными документами по защите	

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	
			Продвинутый уровень	Обучающийся умеет определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации ограниченного доступа, применять отечественные и зарубежные стандарты в области информационной безопасности для оценки защищенности объектов информатизации, пользоваться нормативными документами по защите информации	
		<u>Владеть</u>: - методами формирования требований по	Пороговый уровень	Обучающийся слабо (частично) владеет	**Блок С** – задания практико-ориентированного

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*
		защите информации; – методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов		методами формирования требований по защите информации, методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов	уровня –проекты; – деловая игра - творческое задание (групповое/индивидуальное)
			Базовый уровень	Обучающийся с небольшими затруднениями и владеет методами формирования требований по защите информации, методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов	
			Продвинутый уровень	Обучающийся свободно владеет методами формирования требований по защите	

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, методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов	
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.2. Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений	**Знать:** - особенности основных показателей технико-экономического обоснования соответствующих проектных решений по защите информации; - модели оценки ценности информации;	Пороговый уровень	Обучающийся слабо (частично) знает особенности основных показателей технико-экономического обоснования соответствующих проектных решений по защите информации, модели оценки ценности информации	**Блок А –** задания репродуктивного уровня – тестовые задания; – контрольные вопросы
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает особенности	

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*
				основных показателей технико-экономического обоснования соответствующих проектных решений по защите информации, модели оценки ценности информации	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает особенности основных показателей технико-экономического обоснования соответствующих проектных решений по защите информации, модели оценки ценности информации	
		Уметь: -	Пороговый уровень	Обучающийся слабо	**Блок В** – задания реконструктивного

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*
		разрабатывать техническое задание на создание систем безопасности информации ограниченного доступа, проектировать такие системы с учетом требований нормативных документов; - определять перечень информации ограниченного доступа организации, подлежащей защите;		(частично) умеет разрабатывать техническое задание на создание систем безопасности информации ограниченного доступа, проектировать такие системы с учетом требований нормативных документов, определять перечень информации ограниченного доступа организации, подлежащей защите	уровня – письменная работа; – темы рефератов; – тема презентаций.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет разрабатывать техническое задание на создание систем безопасности информации ограниченного доступа, проектировать	

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*
				такие системы с учетом требований нормативных документов, определять перечень информации ограниченного доступа организации, подлежащей защите	
			Продвинутый уровень	Обучающийся умеет разрабатывать техническое задание на создание систем безопасности информации ограниченного доступа, проектировать такие системы с учетом требований нормативных документов, определять перечень информации ограниченного доступа организации, подлежащей защите	
		Владеть: - методами	Пороговый уровень	Обучающийся слабо	**Блок С** – задания практико-

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***
		анализа и обработки исходных данных для проектирования подсистем, средств обеспечения защиты информации		(частично) владеет методами анализа и обработки исходных данных для проектирования подсистем, средств обеспечения защиты информации	ориентированного уровня выполнение проекта; –кейс-задачи; –проекта; –деловая игра.
			Базовый уровень	Обучающийся с небольшими затруднениями владеет методами анализа и обработки исходных данных для проектирования подсистем, средств обеспечения защиты информации	
			Продвинутый уровень	Обучающийся свободно владеет методами анализа и обработки исходных данных для проектирования подсистем, средств обеспечения	

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*
				защиты информации	
ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4.1. Контролирует уровень защищенности в автоматизированных системах	**Знать:** - виды аудита информационной безопасности; – принципы организации автоматизированных систем в соответствии с требованиями по защите информации	Пороговый уровень	Обучающийся слабо (частично) знает виды аудита информационной безопасности, принципы организации автоматизированных систем в соответствии с требованиями по защите информации	**Блок А –** задания репродуктивного уровня – тестовые задания; – контрольные вопросы
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает виды аудита информационной безопасности, принципы организации автоматизированных систем в соответствии с требованиями по защите информации	
			Продвину	Обучающийся	

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*
			тый уровень	с требуемой степенью полноты и точности знает виды аудита информационной безопасности, принципы организации автоматизированных систем в соответствии с требованиями по защите информации	
		<u>Уметь:</u> **-** выявлять уязвимости автоматизированных систем; - проводить мониторинг угроз безопасности автоматизированных систем	Пороговый уровень	Обучающийся слабо (частично) умеет выявлять уязвимости автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем	**Блок В** – задания реконструктивного уровня – письменная работа; – темы рефератов; – тема презентаций.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет выявлять уязвимости автоматизированных систем,	

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*
				проводить мониторинг угроз безопасности автоматизированных систем	
			Продвинутый уровень	Обучающийся умеет выявлять уязвимости автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем	
		Владеть: - методами выявления угроз информационной безопасности автоматизированных систем; - методами диагностики систем защиты автоматизированных систем с использованием различных тестов на проникновение (ПенТестинг)	Пороговый уровень	Обучающийся слабо (частично) владеет методами выявления угроз информационной безопасности автоматизированных систем, методами диагностики систем защиты автоматизированных систем с использованием различных тестов на проникновени	**Блок С** – задания практико-ориентированного уровня выполнение проекта; –кейс-задачи; –проекта; –деловая игра.

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*
				е (ПенТестинг)	
			Базовый уровень	Обучающийся с небольшими затруднениями и владеет методами выявления угроз информационной безопасности автоматизированных систем, методами диагностики систем защиты автоматизированных систем с использованием различных тестов на проникновение (ПенТестинг)	
			Продвинутый уровень	Обучающийся свободно владеет методами выявления угроз информационной безопасности автоматизированных систем, методами диагностики	

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*
				систем защиты автоматизированных систем с использованием различных тестов на проникновение (ПенТестинг)	

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

Для проверки сформированности компетенции ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ОПК-6.2. Подготавливает объект информатизации для прохождения аттестации на соответствие требованиям государственных и ведомственных нормативных документов

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

Тесты типа А.

1. Кто принимает решение об общедоступности информации:

а) Субъект, получающий доступ к такой информации
б) Владелец Интернет-ресурса, на котором размещается информация
в) Обладатель общедоступной информации

2. На какие две категории можно разделить информацию при классификации ее по категории доступа:
а) Открытая и закрытая
б) Общедоступная и конфиденциальная
в) Общедоступная и ограниченного доступа
г) Секретная и несекретная

3. Можно ли относить нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина к информации ограниченного доступа:
а) Да
б) Нет

4. Какая информация отнесена к сведениям конфиденциального характера:

а) Персональные данные

б) Служебная тайна
в) Государственная тайна
г) Общедоступная информация
д) Сведения, связанные с профессиональной деятельностью
е) Информация ограниченного доступа

5. Укажите федеральные органы исполнительной власти, уполномоченные в области безопасности информации:
а) Служба внешней разведки РФ
б) Федеральная служба по техническому и экспортному контролю РФ
в) Федеральная служба охраны РФ
г) Федеральная служба безопасности РФ

6. Определите процедуру, которая должна быть проведена с целью оценки соответствия требованиям по безопасности информации принятых на объекте мер по защите информации:
а) Сертификация
б) Аттестация
в) Аккредитация
г) Лицензирование

7. Имеет ли право владелец Интернет-ресурса единолично принимать решение об общедоступности информации, размещаемой пользователем на ресурсе:

а) Да
б) Нет

8. Выберите виды информации при классификации ее по категориям доступа:

а) Открытая информация
б) Общедоступная информация
в) Информация ограниченного доступа
г) Секретная информация
д) Информация свободного доступа
е) Конфиденциальная информация
ж) Свободно распространяемая информация

9. Информация какого вида, в соответствие с федеральными законами, не может быть отнесена к информации ограниченного доступа:

а) Государственная тайна
б) Информация о состоянии окружающей среды
в) Информация о частной жизни гражданина
г) Тайна голосования
д) Нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина
е) Тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

10. Какая информация не относится к сведениям конфиденциального характера, исходя из «Перечня сведений конфиденциального характера», утвержденным Указом Президента РФ от 6 марта 1997 г. N 188:

а) Персональные данные
б) Государственная тайна
в) Тайна следствия и судопроизводства
г) Общедоступная информация
д) Служебная тайна
е) Информация ограниченного доступа

Тесты типа В.

11. ФСТЭК России - это:

а) Федеральная служба по техническому и экспортному контролю, осуществляющая защиту безопасности личности, общества и государства от внешних угроз
б) Федеральная служба по техническому и экспертному контролю, осуществляющая организацию деятельности государственной системы технической защиты информации

в) Федеральная служба по техническому и экспортному контролю, осуществляющая организацию деятельности государственной системы противодействия техническим разведкам и технической защиты информации
г) Федеральная служба по техническому и экспертному контролю, осуществляющая защиту безопасности личности, общества и государства от внешних угроз

12. Оценка соответствия объекта информатизации требованиям безопасности информации осуществляется в ходе:
а) Лицензирования
б) Сертификации
в) Аккредитации
г) Аттестации

13. Паспортные данные (ФИО, прописка, место и дата рождения, семейное положение, серия и номер паспорта) клиентов компании, оказывающей услуги связи это:
а) Информация ограниченного доступа
б) Общедоступная информация
в) Служебная тайна
г) Персональные данные

14. Аттестация объектов информатизации по требованиям безопасности информации это:
а) Обеспечение защиты информации на объекте информатизации
б) Соответствие комплекса мероприятий по защите информации, проведенного на объекте информатизации, требованиям по безопасности информации
в) Мероприятия по обеспечению безопасности при обработке информации на объекте информатизации
г) Процедура подтверждения правильности выбора объекта информатизации

15. К какой государственной системе относится аттестация:
а) Лицензирования
б) Обеспечения государственной безопасности
в) Сертификации средств защиты информации
г) Защиты информации

16. Станут ли персональные данные общедоступной информацией при размещении ее в социальных сетях?
а) Нет
б) Да

17. Кто может выступать обладателем информации?

а) Индивидуальный предприниматель
б) Российская Федерация
в) Физическое лицо
г) Субъект Российской Федерации

18. Включена ли государственная тайна в «Перечень сведений конфиденциального характера», утвержденный Указом Президента РФ от 6 марта 1997 г. N 188?
а) Да
б) Нет

А2. Контрольные вопросы

1. Перечислите основные этапы построения КСЗИ.
2. Назовите ГОСТ с учётом которых должны быть разработаны требования к системе защиты информации.
3. Перечислите основные понятия которые будут определены при проектировании КСЗИ.
4. Перечислите процессы выполняемые при обеспечении защиты информации в ходе эксплуатации аттестованной информационной системы.
5. Что входит в состав защищаемой информации?

Блок В. Задания реконструктивного уровня («уметь»)

В1. Письменная работа

Раскрыть особенности следующих объектов безопасности в соответствии с Федеральным законом "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ:

- Правовое обеспечение безопасности информации в форме сведений;
- Правовое обеспечение безопасности информации в форме сообщений;
- Правовое обеспечение безопасности информационной инфраструктуры;
- Правовое обеспечение безопасности правового статуса субъекта информационной сферы.

В2. Темы рефератов

1. Виды угроз информации.
2. Формальная модель нарушителя.
3. Каналы несанкционированного доступа.
4. Методы противодействия несанкционированному доступу.
5. Особенность внедрения комплексной системы защиты информации.

В3. Темы презентаций

1. Свойства информационной системы, влияющие на вопросы информационной безопасности.
2. Основные принципы организации комплексного обеспечения защиты информации.
3. Концепция разработки комплексной системы защиты информации.
4. Требования к комплексной системе защиты информации.
5. Информация как объект защиты: категории, определения.

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

С1. Кейс-задача.

Описание ситуации

В одной из компаний был зафиксирован следующий инцидент: при увольнении с работы системный администратор украл разрабатываемый в компании программный продукт и передал его конкурентам, которые выпустили программу на рынок под своим товарным знаком. Кроме этого, он внес изменения в информационную систему, в результате которых после его ухода функционирование определенных ее компонентов было нарушено. Привлечь администратора к ответственности в данном случае оказалось невозможно, так как, во-первых, не выполнялась регистрация его действий, во-вторых, администратор мог удалить все доказательства своих неправомерных действий и, в-третьих, не была налажена процедура сбора улик об инциденте.

Задание:

1. Определите возможные причины инцидента и степень ответственности сотрудника.

2. Определите меры, направленные на предотвращение повторных инцидентов.

3. Подготовьте проекты соответствующих документов.

С2. Проект

1. Выбрать из списка ниже организацию и написать по ней отчёт, содержащий общие сведения о ней, о ее деятельности и организационной структуре:

- Автосалон;
- Частное охранное предприятие;
- Магазин бытовой техники;
- Администрация района (города);
- ВУЗ (ССУЗ);
- Коммунальная служба (ЖКХ);
- Министерства (ведомства);
- РОВД (ГУВД, ЛУВД, ОВО);

- Прокуратура района (города);
- Следственный комитет района (города);
- Организация в сфере промышленности: нефтяная компания, энергокомпания, завод (на выбор);
- Судебные приставы района (города);
- Суд района (города);
- Федеральные органы власти: ФНС, ФАС, ПФ РФ (на выбор);
- Организация по грузоперевозкам;
- Компьютерный супермаркет;
- Компьютерные курсы;
- Развлекательный комплекс, организация в сфере оказания развлекательных услуг (на выбор);
- Строительная компания;
- Торговый дом (мебельный салон);
- Больница, поликлиника, госпиталь, санаторий, роддом(на выбор);
- Банк;
- Детский сад, школа (на выбор);
- Турагентство;
- Общественная, политическая организация;
- Рекламная компания;
- Ресторан;
- Федерация спорта;
- Средство массовой информации;
- Агентство недвижимости;
- Транспортная компания,
- ЖД-вокзал (автовокзал).

2. Изучить стандарты ГОСТ Р ИСО/МЭК 15408-1-2008, ГОСТ Р ИСО/МЭК 15408-2-2008, ГОСТ Р ИСО/МЭК 27001-2006, ГОСТ Р ИСО/МЭК 17799-2005.

3. Построить алгоритм анализа информации, циркулирующей в корпоративной информационной системе.

4. Проанализировать информацию, циркулирующей в корпоративной информационной системе предприятия.

5. Построить полную диаграмму информационных потоков предприятия.

С3. Деловая игра

У менеджера компании «Аскона» есть личный электронный ящик, также что он пользуется социальными сетями (Вконтакте, Одноклассники и т.д). При этом он закрывает браузер не нажимая кнопку «выход», использует Google Chrome, имеет 1-2 несложных пароля на все ресурсы, выходит в сеть в основном с рабочего места иногда из дома. Менеджер – коммуникабельная, активная девушка, участница форумов. На сайтах регистрируется под ником ***

Студенты делятся на 2 группы: «Защитники» (Админы) и «Злоумышленники» (Хакеры).

Каждая команда сообразно своим интересам определяет для менеджера:

- риски по аспектам информационной безопасности: целостность, доступность, конфиденциальность;
- уязвимости;
- угрозы;
- уровень неприемлемого ущерба;
- контрмеры - политику безопасности (для защитников);
- порядок атак (для злоумышленников).

После обсуждения, студентам сообщается имя девушки и её ник (он виртуальный). Студенты выходят в Интернет, и кто первый успеет (найти почту, поменять пароли, сменить данные, чтоб не нашли другие и пр.), тот и победил.

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Свойства информационной системы, влияющие на вопросы информационной безопасности.
2. Основные принципы организации комплексного обеспечения защиты информации.
3. Концепция разработки комплексной системы защиты информации.
4. Требования к комплексной системе защиты информации.
5. Информация как объект защиты: категории, определения.
6. Виды угроз информации.
7. Формальная модель нарушителя.
8. Каналы несанкционированного доступа.
9. Методы противодействия несанкционированному доступу.

Для проверки сформированности компетенции ОПК-12
Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

ОПК-12.2. Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

Тесты типа А.

1. Выберите из ниже предложенного пассивные технические мероприятия (возможно несколько вариантов):

а) Назначение ответственного за защиту информации в организации
б) Улучшение звукоизолирующих свойств помещения посредством облицовки стен панелями
в) Экранирование технических средств обработки информации
г) Использование системы защиты информации от несанкционированного доступа

2. Выберите объект испытаний при проведении процедуры аттестации:

а) Индивидуальный предприниматель
б) Средство контроля эффективности защиты информации
в) Помещение для проведения конфиденциальных переговоров
г) Юридическое лицо

3. Государственная система защиты информации включает в себя:

а) Подсистему сертификации СЗИ и подсистему лицензирования в области ЗИ
б) Подсистему сертификации СЗИ и подсистему аттестации ОИ
в) Подсистему лицензирования в области ЗИ и подсистему аттестации ОИ

4. Выберите из ниже предложенного объекты информатизации, подлежащие защите:

а) Автоматизированные системы
б) Средство защиты информации
в) Система размножения документов
г) Средство контроля эффективности защиты информации

5. Выберите объект испытаний при проведении процедуры лицензирования:

а) Объект информатизации
б) Средство защиты информации
в) Автоматизированная система
г) Юридическое лицо

6. Выберите из ниже предложенного организационные мероприятия (возможно несколько вариантов):

а) Классификация автоматизированных систем
б) Установка шумоизолирующих прокладок на дверь
в) Составление перечня информации, подлежащей защите
г) Установка сертифицированной по требованиям безопасности информации операционной системы

7. Выберите объект испытаний при проведении процедуры сертификации:

а) Объект информатизации
б) Изделие

в) Помещение для ведения конфиденциальных переговоров
г) Индивидуальный предприниматель

8. К какому типу мер по защите информации относится установка уплотнителей в дверном проеме защищаемого помещения?
а) Организационная
б) Активная техническая
в) Строительная
г) Пассивная техническая

9. В какой процедуре участвует третья сторона – испытательная лаборатория?
а) Аттестация
б) Аккредитация
в) Лицензирование
г) Сертификация

10. Специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности это:
а) Аттестат аккредитации
б) Сертификат соответствия
в) Лицензия
г) Аттестат соответствия
д) Заключение
е) Предписание

Тесты типа В.

11. Выберите виды мероприятий по защите информации:
а) Технические пассивные
б) Активные
в) Организационные пассивные
г) Технические активные
д) Организационные активные
е) Пассивные

12. Какой орган государственной власти является правопреемником Гостехкомиссии России?
а) ФАПСИ
б) ФСО
в) ФСТЭК
г) ФСБ

13. По результатам проведения комплекса организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации

соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации выдается:

а) Аттестат соответствия
б) Аттестат аккредитации
в) Сертификат соответствия
г) Лицензия
д) Заключение
е) Предписание

14. Какие меры защиты информации предусматривают использование конструктивных решений и технологических особенностей обработки информации ограниченного доступа на объектах информатизации?

а) Активные
б) Пассивные
в) Организационные пассивные
г) Организационные активные
д) Технические пассивные
е) Технические активные

15. При необходимости подтверждения соответствия системы активной защиты информации установленным требованиям проводится процедура:

а) Аттестации
б) Лицензирования
в) Сертификации
г) Аккредитации

16. Можно ли в качестве активной технической меры выбрать установку сертифицированной антивирусной программы?

а) Да
б) Нет

17. Оценка возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями проводится при:

а) Сертификации
б) Аттестации
в) Лицензировании

18. Выберите стороны, участвующие в процессе лицензирования:

а) Юридическое лицо и ФСТЭК России
б) Орган по аттестации и испытательная лаборатория
в) Заявитель и орган по аттестации
г) Заявитель и юридическое лицо

д) Физическое лицо и орган по сертификации

А2. Контрольные вопросы

1. Какие модели комплексной системы защиты информации?
2. Какие компоненты комплексной системы защиты информации вы знаете?
3. Что из себя представляет комплексная система защиты информации?
4. Назовите регламент обеспечения информационной безопасности.
5. В чем заключается модель безопасности Белла – Ла Падулы?

Блок В. Задания реконструктивного уровня («уметь»)

В1. Письменная работа

- Нормативные основы и основные понятия управления инцидентами ИБ.
- Схема управлением инцидентами.
- Этапы менеджмента инцидентами ИБ.
- Что такое информационная система?
- Из каких задач состоит комплексная система защита информации?

В2. Темы рефератов

1. Подходы к разработке автоматизированных информационных систем и систем защиты информации в их рамках.
2. Модели управления доступом: классификация и краткая характеристика.
3. Модель безопасности Белла – Ла Падулы.
4. Компоненты комплексной системы защиты информации.
5. Регламент обеспечения информационной безопасности.

В3. Темы презентаций

1. Особенности работы подразделения информационной безопасности.
2. Защита автоматизированной информационной системы от случайных угроз.
3. Методы зашиты информации от шпионажа.
4. Порядок работы с информационными ресурсами.
5. Методы защиты от несанкционированного изменения информации.

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

С1. Деловая игра.

Описание ситуации

Ваша группа является частью команды организации-разработчика, которая участвует в проекте создания комплексной системы защиты информационной системы. Ваша задача заключается в сборе информации о объекте автоматизации, определении состава защищаемой информации, классификации этой информации, в том числе по видам тайн и степеням конфиденциальности. По итогам работы ваша группа составляет сведения об основные информационных пакетах,

классифицируемых по вышеуказанному признаку. По итогам вашей работы будут формулироваться дальнейшие требования к проектируемой системе, которые впоследствии потребуется внести в техническое задание на создание системы.

Для решения задачи вам необходимо:

1. Проанализировать сведения об предложенной информационной системе.
2. Составить перечень, состав и степень конфиденциальности так называемых информационных пакетов. Информационный пакет – условное обозначения некоторой совокупности сведений, документов и т.п., которые можно объединить по какому-либо признаку. Например, назовем информационный пакет «Анкетные данные». Определим состав пакета: анкета сотрудника, анкетные данные сотрудника. Для определения степени конфиденциальности воспользуемся материалами законодательных актов и будем опираться на схему классификации информации по степени конфиденциальности и видам тайн:

Обучающиеся делятся на группы (по 4-5 человек) и определяют роли среди членов группы:

- руководитель:
  - распределяет роли и записывает в оценочном листе группы;
  - наблюдает за работой членов группы,
  - участвует с остальными членами группы в обсуждении материалов кейса,
  - выставляет оценку каждому участнику группы за выполненную работу в оценочном листе группы;
- ответственный за оформление отчета согласно рекомендациям оформляет отчет по работе с кейсами и сдает руководителю;
- остальные члены группы совместно с руководителем и ответственным за оформление отчета работают с материалами кейса.

С2. Проект

Цель выполнения проекта: Ознакомиться с особенностями межсетевых экранов: установка, настройка, тестирование на блокирование стороннего пакета.

Задание: Определить степень влияния межсетевых экранов на блокирование стороннего пакета. Данные анализа занести в таблицу 2.

Результат проекта: Результаты проекта представляют собой сводные данные межсетевых экранов по указанному заданию, а также презентация, отражающая основные этапы выполнения задания.

Критерии оценки:

1. Полнота проведенного анализа.
2. Полнота обоснования результатов и выводов.
3. Подготовка презентации выполненного проекта.

Таблица 1. Перечень межсетевых экранов(на выбор)

№	Наименование
1.	ComodoInternetSecurityPremium
2.	Privatefirewall
3.	KasperskyInternetSecurity
4.	OutpostSecuritySuitePro
5.	VirusBusterInternetSecuritySuite
6.	JeticoPersonalFirewall
7.	ESET SmartSecurity
8.	ZoneAlarmExtremeSecurity
9.	Total Defense Internet Security Suite
10.	avast! InternetSecurity
11.	Dr.WebSecuritySpace
12.	AviraInternetSecurity
13.	BitdefenderTotalSecurity
14.	NortonInternetSecurity
15.	PandaGlobalProtection
16.	McAfeeTotalProtection
17.	Ad-AwareTotalSecurity
18.	AVG InternetSecurity

Таблица 2.Пример выполнения работы

Level 1		
Имя теста	Ваш Вариант	
	Первое тестирование (МЭ установлен с настройками «по умолчанию»)	Второе тестирование (настройки МЭ изменены с учётом проваленных тестов)
Yalta.exe	+	+
Wallbreaker1.exe	+	+
Toolekay.exe	+	+
Leaktest.exe	-	+
Kill2	**и т.д.**	**и т.д.**

Kill1		
Echotest		
Coat		
Breakout2		
Level 2		
Awft1		
Dnstest		
Ghost		
Jumper		
Kill3		
Kill3d		
Kill6		
Wallbreaker3		
Wallbreaker4		
Level 3		
Awft3		
Awft4		
Dnstester		
Kernel1		
Kill3f		
Kill4		
Kill7		
Sss2		
Suspend1		
Thermite		
Level 4		
Copycat		
Cpil		
Cpilsuite1		
Kernel1b		
Keylog1		
Kill3e		
Kill8		
Kill9		
Sss		
Suspend2		
Level 5		
Breakout1		
Cpilsuite2		
Crash1		
Crash2		

Crash3		
Crash4		
Kernel2		
Kernel3		
Keylog2		
Kill3c		
Kill3d		
Vbstest		
Level 6		
Cpilsuite3		
Crash5		
Crash6		
Ddetest		
Echotest2		
Firehole		
Flank		
Kernel4		
Keylog3		
Keylog4		
Kill10		
Kill11		
Runner		
Level 7		
Bitstest		
Firehole2		
Keylog5		
Keylog6		
Kill12		
Osfwbypass		
Runner2		
Schedtest		
Sss3		
Level 8		
Kernel4b		
Kernel5		
Keylog7		
Kill5		
Newclass		
Schedtest2		
socksnif		
Ssss4		

Level 9		
Crash7.exe		
Fileacc1.exe		
Filewri4.exe		
Filectl.exe		
Level 10		
bsobhook		

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Особенность внедрения комплексной системы защиты информации.
2. Подходы к разработке автоматизированных информационных систем и систем защиты информации в их рамках.
3. Модели управления доступом: классификация и краткая характеристика.
4. Модель безопасности Белла – Ла Падулы.
5. Компоненты комплексной системы защиты информации.
6. Регламент обеспечения информационной безопасности.
7. Особенности работы подразделения информационной безопасности.
8. Защита автоматизированной информационной системы от случайных угроз.
9. Методы зашиты информации от шпионажа.
10. Порядок работы с информационными ресурсами.
11. Методы защиты от несанкционированного изменения информации.
12. Контрольной-испытательный стенд и правила его применения.
13. Система защиты программных средств от копирования и исследования.
14. Вредоносное программное обеспечение: определения, классификация, методы противодействия.
15. Структура межсетевых экранов
16. Системы обнаружения и предотвращения вторжений. Преимущества и недостатки.
17. Алгоритм работы и примеры систем обнаружения и предотвращения вторжений.

Для проверки сформированности компетенции ОПК-4.4
Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем

ОПК-4.4.1. Контролирует уровень защищенности в автоматизированных системах

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

Тесты типа А.

1. Какую лицензию должна получить испытательная лаборатория для проведения работ по сертификации средств защиты информации, используемых на объектах информатизации, обрабатывающих информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну?
   а) На проведение работ, связанных с созданием средств защиты информации
   б) На осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну
   в) На деятельность по технической защите конфиденциальной информации
   г) На деятельность по разработке и производству средств защиты конфиденциальной информации

2. Является ли лицензиат, имеющий лицензию на деятельность по ТЗКИ, органом по аттестации объектов информатизации, предназначенных для обработки информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну?
   а) Да
   б) Нет

3. Какой документ необходим органу по аттестации для проведения работ по аттестации ОИ по требованиям безопасности информации при обработке информации, не содержащей сведения, составляющие государственную тайну:
   а) Сертификат соответствия
   б) Лицензия на разработку и производство СЗКИ
   в) Аттестат аккредитации
   г) Аттестат соответствия
   д) Лицензия на осуществление деятельности по ТЗКИ

4. Какая организация из нижеперечисленных при наличии соответствующего разрешительного документа может проводить сертификационные испытания средств защиты информации:
   а) Испытательная лаборатория
   б) Орган по аттестации
   в) Лицензиат, имеющий лицензию на ТЗКИ
   г) Заявитель

5. Выберите из ниже предложенного функции органа по аттестации:
   а) Учет аттестованных ОИ
   б) Приостановка действия «Аттестата соответствия…»
   в) Проведение периодического контроля за состоянием защищенности информации на аттестованных ОИ
   г) Выдача предписания на приостановление работ на объектах информатизации

6. Кому испытательная лаборатория имеет право направить протокол о проведенных испытаниях средств защиты информации:

а) Органу по аттестации
б) Федеральному органу по сертификации средств защиты информации
в) Никому, оставляет их у себя
г) Производителю средства защиты информации, подавшему заявку на сертификацию
д) Направляет в любую организацию по запросу

7. Выберите из нижеперечисленного задачи, стоящие перед заявителем на аттестацию ОИ для обработки информации ограниченного доступа:

а) Получение лицензии на деятельность по разработке и производству СЗКИ
б) Проведение аттестационных испытаний ОИ
в) Подготовка необходимых документов и технических средств для проведения аттестации
г) Установка и настройка сертифицированных СЗИ
д) Извещение органа по аттестации об изменениях, возникающих на ОИ и способных повлечь за собой снижение заданного уровня защищенности

8. Необходим ли органу по аттестации аттестат аккредитации для проведения работ по аттестации ОИ по требованиям безопасности информации при обработке информации, не содержащей сведения, составляющие государственную тайну:

а) Да
б) Нет

9. Кто выдает предписания на приостановление работ на аттестованном объекте информатизации?

а) ФСТЭК России
б) Орган по аттестации
в) Лицензиат, имеющий лицензию на ТЗКИ
г) Заявитель

10. Может ли испытательная лаборатория, получившая Лицензию на деятельность по ТЗКИ, проводить работы по аттестации объектов информатизации заявителя?

а) Да
б) Нет

Тесты типа В.

11. Выберите функции, возложенные на ФСТЭК России по вопросам аттестации ОИ (возможно несколько вариантов):

а) Осуществляет периодический контроль за состоянием защищенности информации на аттестованных объектах информатизации заявителя.
б) Выдает лицензии на осуществление деятельности по ТЗКИ.
в) Осуществляет работы по аттестации ОИ по заявкам от заявителей.
г) Выдает предписания на приостановление работ на ОИ.
д) Рассматривает апелляции по вопросам аттестации ОИ по требованиям безопасности информации.
е) Осуществляет подготовку объекта информатизации заявителя к проведению работ по аттестации.

12. Имеет ли право заявитель обратиться к органу по аттестации за помощью по подготовке объекта информатизации к аттестации:
а) Нет, заявитель должен самостоятельно готовить объект информатизации к аттестации
б) Да, при условии получения разрешения от ФСТЭК России
в) Да, оплатив дополнительный объем работ органу по аттестации
г) Нет, это не предусмотрено законодательством Российской Федерации в области защиты информации

13. Может ли испытательная лаборатория, получившая Лицензию на деятельность по ТЗКИ, проводить работы по аттестации объектов информатизации заявителя?
а) Да
б) Нет

14. Выберите функции испытательной лаборатории:
а) Осуществляет установку средств защиты информации на объектах информатизации.
б) Проводит оценку эффективности средств защиты информации, установленных на объектах информатизации.
в) Проводит сертификацию средств защиты информации.
г) Выдает протоколы испытаний с заключением о соответствии или несоответствии средств защиты информации установленным требованиям.
д) Осуществляет настройку средств защиты информации в соответствии с требованиями, предъявляемыми к системе защиты информации.

15. Какую лицензию должен получить орган по аттестации для проведения работ по аттестации объектов информатизации?
а) На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации)
б) На деятельность по технической защите конфиденциальной информации.
в) На проведение работ, связанных с созданием средств защиты информации.
г) На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны

16. Выберите верный перечень органов и организаций, входящих в организационную структуру системы аттестации объектов информатизации:

а) ФСТЭК России, лицензиаты в области ТЗКИ, заявители
б) Федеральный орган по сертификации средств защиты информации, испытательные лаборатории.
в) ФСТЭК России, органы по аттестации, испытательные лаборатории, заявители
г) Федеральный орган по аттестации ОИ по требованиям безопасности информации, органы по аттестации, заявители.

17. Чем определены сроки и последовательность прохождения процедур для получения лицензии на деятельность по разработке и производству средств защиты конфиденциальной информации?

а) Федеральным законом
б) Постановлением Правительства
в) Руководящим документом
г) Административным регламентом
д) Нормативным документом
е) Положением
ж) ГОСТом
з) Рекомендациями по стандартизации

18. Какого вида деятельности нет в лицензии на деятельность по технической защите конфиденциальной информации?

а) Услуги по мониторингу информационной безопасности средств и систем информатизации.
б) Услуги по проектированию в защищенном исполнении средств и систем информатизации.
в) Услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации.
г) Услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации защищаемых помещений.
д) Услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации
е) Услуги по проведению специсследований на побочные электромагнитные излучения и наводки технических средств обработки информации

А2. Контрольные вопросы

1. Что такое SQL-инъекция?
2. Что из себя представляет дискреционная модель управления доступом?
3. Что из себя представляет мандатная модель управления доступом?
4. Что такое тотальный перебор?

5. Что такое роль? привилегия?

Блок В. Задания реконструктивного уровня («уметь»)

В1. Практическая работа

Работа с настройками ролей и разграничений доступа в СУБД MS SQLServer. Создание пользователей и ролей в СУБД MS SQL Server.
Цель работы: Ознакомиться с настройками ролей, схемой данных и разграничений доступа в СУБД MS SQLServer. Ознакомиться с особенностями создания пользователей, ролей, схемой данных и разграничений доступа в СУБД MS SQL Server.

В2. Темы рефератов

1. Архитектура защиты СУБД MS SQLServer. Пользователи, группы и разрешения.
2. Способы защиты в СУБД MS SQLServer. Парольная защита баз данных.
3. Шифрование. Параметры запуска. Защита на уровне пользователя.
4. Система безопасности MS SQLServer 2008 выше. Шестиуровневая модель системы безопасности MS SQLServer.
5. Планирование безопасности баз данных. Привилегии безопасности. Виды привилегий. Привилегии доступа.
6. Целостность данных. Типы целостности. Структурная целостность базы данных.
7. Типы структурных проблем. Управление структурными проблемами. Проверка базы данных. Использование памяти.

В3. Темы презентаций

1. Семантическая целостность данных. Целостность объектов. Уникальные ограничения.
2. Типы данных. Типы данных, определяемые пользователем. Значения по умолчанию.
3. Резервное копирование. Полная копия. Разностная копия. Копия журнала транзакций.
4. Резервное копирование файлов и групп. Планирование стратегии резервного копирования.
5. Репликация баз данных. Задача агентов.
6. Методы репликации. Репликация снимков.

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

С1. Проект

Средства идентификации и аутентификации в СУБД MS SQL Server

1. Для доступа к SQL Server необходимо создать 4 учетные записи (логины): *«Администратор БД»*, *«Сотрудник отдела кадров»*, *«Сотрудник отдела продаж»*, *«Сотрудник отдела поставок»*;

Учетную запись «Администратор» необходимо наделить привилегиями системного администратора (с помощью системной роли);

Написать SQL-скрипты для получения следующей информации:

1. Секретный идентификатор, имя, хэш пароля определенной учетной записи;

2. Список всех учетных записей сервера;

3. Список всех учетных записей сервера, обладающих правами администратора;

Написать SQL-скрипты для выполнения следующих действий с учетной записью SQL-сервера:

1. Блокировка учетной записи (временное приостановление действия);

2. Разблокировка учетной записи;

3. Изменение пароля учетной записи;

4. Изменение БД по умолчанию;

5. Удаление учетной записи;

Написать SQL-скрипты для выполнения следующих действий с учетной записью операционной системы (ОС):

1. Регистрация учетной записи ОС в качестве учетной записи в MS SQL Server;

2. Отмена регистрации учетной записи ОС в качестве учетной записи в MS SQL Server;

3. Запрет подключений учетной записи ОС в качестве учетной записи в MS SQL Server;

Для каждой учетной записи, созданной в 1 пункте, кроме «Администратор БД» необходимо добавить пользователя в вашу БД.

<u>С2. Творческое задание (групповое/индивидуальное)</u>

Необходимо создать кроссворд, состоящий из следующих вопросов и ответов (в именительном падеже):

1. Иерархическая база данных может быть отображена в виде…… *(Дерево)*
2. Основной способ представления реляционной базы данных……*(Таблица)*
3. Для его создания используют построитель….. *(Выражений)*
4. Позволяет изменить структуру базы данных…… *(Конструктор)*
5. Определяет принцип отбора данных…… *(Условие)*
6. ……ввода облегчает набор данных. Например, номера телефона, индекса. *(Маска)*
7. Определяет главное поле. *(Ключ)*
8. Программа, позволяющая создавать и обрабатывать базы данных. *(СУБД)*

9. Можно установить между таблицами. *(Связь)*
10. Позволяет просматривать все записи. *(Фильтр)*
11. Представление данных по одной записи. *(Форма)*
12. Тип данных. *(Логический)*
13. Подготовка базы данных к печати. *(Отчет)*
14. Выборка данных по условию с возможностью сохранения. *(Запрос)*
15. Набор данных одного типа в структуре реляционной базы данных. *(Поле)*
16. Процесс обнаружения нужных данных. *(Поиск)*
17. Набор данных разного типа об одном объекте. *(Запись)*

С3. Кейс-задача

Описание ситуации

Ваша группа является частью команды организации-разработчика, которая участвует в проекте создания комплексной системы защиты информационной системы. Ваша задача заключается в сборе информации о объекте автоматизации, определении состава защищаемой информации, классификации этой информации, в том числе по видам тайн и степеням конфиденциальности. По итогам работы ваша группа составляет сведения об основные информационных пакетах, классифицируемых по вышеуказанному признаку. По итогам вашей работы будут формулироваться дальнейшие требования к проектируемой системе, которые впоследствии потребуется внести в техническое задание на создание системы.

Объектом обследования является ИС «Поликлиника».

Функции системы:

1) введение справочника данных о пациенте,

2) ведение справочника сотрудников поликлиники,

3) введение справочников диагнозов и обследований,

4) запись на прием к врачу (как регистратором в поликлинике, так и пациентом через Интернет-сервис);

5)поиск пациентов, их диагнозов, результатов обследования,

6)подготовка к печати статистических данных;

7)предоставление сведений о расписании врачей;

8)предоставление сведений о поликлинике, руководстве поликлиники, режиме работы.

Пользователи системы:

1)Регистраторы;

2)Главный врач;

3)Врачи;

4)Бухгалтерия;

5)Статистическая служба;

6)Пациенты.

Задание:

1.Определите возможные информационные пакеты.

2.Определите степень конфиденциальности информационных ресурсов, входящих в состав пакета.

3.Перечислите категории конфиденциальности информации, которые в данной системе отсутствуют. Укажите подтверждающие законодательные акты (№ ФЗ, указа, статья).

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Привилегии и модели разграничения доступа.
2. Дискреционное управление доступом. Ролевое управление доступом.
3. Параллельное выполнение транзакций.
4. Процесс получения доступа пользователя к БД в СУБД.
5. Задача обеспечения ИБ БД. Проблемы. Решение. Недостатки.
6. Особенности СУБД как объекта защиты ИБ БД. Задача обеспечения конфиденциальности, целостности, доступности информации.

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.

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 –	85 и ≥	70 – 84	51 – 69	0 – 50

балльная шкала				
4 – балльная шкала	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»

Шкала оценок при текущем контроле успеваемости по различным показателям

Показатели оценивания сформированности компетенций	***Баллы***	***Оценка***
Выполнение лабораторных работ	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение проекта	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Проведение деловой игры	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение творческого задания	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение и публичная защита реферата	0-3	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение и публичная демонстрация презентации	0-2	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

В графе «Показатели оценивания сформированности компетенций» приводятся формы текущего контроля успеваемости в соответствии с рабочей программой конкретной дисциплины и видами оценочных средств согласно подразделу 1.2.

В графе «Баллы» указываются баллы в соответствии с технологической картой конкретной дисциплины.

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»

Выбирается форма промежуточной аттестации по дисциплине в

соответствии с учебным планом по направлению подготовки.

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

Процедура оценивания – порядок действий при подготовке и проведении аттестационных испытаний и формировании оценки.

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.
- Время подготовки ответа при сдаче зачета/экзамена в устной форме должно составлять не менее 40 минут (по желанию обучающегося ответ может быть досрочным). Время ответа – не более 15 минут.
- При подготовке к устному экзамену экзаменуемый, как правило, ведет записи в листе устного ответа, который затем (по окончании экзамена) сдается экзаменатору.
- При проведении устного экзамена экзаменационный билет выбирает сам экзаменуемый в случайном порядке.
- Экзаменатору предоставляется право задавать обучающимся дополнительные вопросы в рамках программы дисциплины текущего семестра, а также, помимо теоретических вопросов, давать задачи, которые изучались на практических занятиях.

- Оценка результатов устного аттестационного испытания объявляется обучающимся в день его проведения. При проведении письменных аттестационных испытаний или компьютерного тестирования – в день их проведения или не позднее следующего рабочего дня после их проведения.
- Результаты выполнения аттестационных испытаний, проводимых в письменной форме, форме итоговой контрольной работы или компьютерного тестирования, должны быть объявлены обучающимся и выставлены в зачётные книжки не позднее следующего рабочего дня после их проведения.

Итоговой формой контроля по дисциплине является экзамен, проводимый в виде письменного ответа на заданный вопрос. Каждому студенту предлагается 2 вопроса, каждый из которых оценивается максимум на 15 баллов. При оценке ответа на вопрос оценивается полнота ответа, точность формулировок, правильное цитирование соответствующих законодательных актов, наличие иллюстративных примеров.

Оценивание выполнения тестов

Шкала оценок	***Показатели***	***Критерии***
Отлично (высокий уровень сформированности компетенции)	1. *Полнота выполнения тестовых заданий;* 2. *Своевременность выполнения;* 3. *Правильность ответов на вопросы;* 4. *Самостоятельность тестирования;* 5. *и т.д.*	*Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос*
Хорошо (достаточный уровень сформированности компетенции)		*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.*
Удовлетворительно (приемлемый уровень сформированности компетенции)		*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.*
Неудовлетворительно (недостаточный уровень сформированности компетенции)		*Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).*

Оценивание выполнения рефератов

Шкала оценок	*Показатели*	*Критерии*
Отлично (высокий уровень сформированности компетенции)	*1. Полнота выполнения рефератов;* *2. Своевременность выполнения;* *3. Правильность ответов на вопросы;* *4. и т.д.*	*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, даны правильные ответы на дополнительные вопросы.*
Хорошо (достаточный уровень сформированности компетенции)		*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; на дополнительные вопросы при защите даны неполные ответы.*
Удовлетворительно (приемлемый уровень сформированности компетенции)		*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.*
Неудовлетворительно (недостаточный уровень сформированности компетенции)		*Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы*

Оценивание выполнения презентаций

Шкала оценок	*Показатели*	*Критерии*
Отлично (высокий уровень сформированности компетенции)	*1. Полнота выполнения презентаций;* *2. Своевременность выполнения;* *3. Правильность ответов на вопросы;* *4. и т.д.*	*Выполнены все требования к составлению презентаций: дизайн слайдов, логика изложения материала, текст хорошо написан и сформированные идеи ясно изложены и структурированы*
Хорошо (достаточный уровень сформированности		*Основные требования к презентациям выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала;*

компетенции)		*отсутствует логическая последовательность в суждениях; не выдержан объем презентации*
Удовлетворительно (приемлемый уровень сформированности компетенции)		*Имеются существенные отступления от требований к презентациям. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании презентаций или при ответе на дополнительные вопросы.*
Неудовлетворительно (недостаточный уровень сформированности компетенции)		*Тема презентации не раскрыта, обнаруживается существенное непонимание проблемы*

Оценивание решения кейс-задач

Шкала оценок	***Показатели***	***Критерии***
Отлично (высокий уровень сформированности компетенции)	*1. Полнота решения кейс-задач;* *2. Своевременность выполнения;* *3. Правильность ответов на вопросы;* *4. и т.д.*	*Основные требования к решению кейс-задач выполнены. Продемонстрировано умение анализировать ситуацию и находить оптимальное количества 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;*
Хорошо (достаточный уровень сформированности компетенции)		*Основные требования к решению кейс-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*
Удовлетворительно (приемлемый уровень сформированности компетенции)		*Имеются существенные отступления от решения кейс-задач. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат*
Неудовлетворительно		*Задача кейса не раскрыта, обнаруживается существенное*

(недостаточный уровень сформированности компетенции)		*непонимание проблемы*

Оценивание ответов на устные и письменные вопросы

Шкала оценок	***Показатели***	***Критерии***
Отлично (высокий уровень сформированности компетенции)	*1. Полнота данных ответов;* *2. Аргументированность данных ответов;* *3. Правильность ответов на вопросы;* *4. и т.д.*	*Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные. Изложение материала последовательно и правильно.*
Хорошо (достаточный уровень сформированности компетенции)		*Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.*
Удовлетворительно (приемлемый уровень сформированности компетенции)		*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.*
Неудовлетворительно (недостаточный уровень сформированности компетенции)		*Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал; отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.*

Оценивание выполнение проектов

Шкала оценок	***Показатели***	***Критерии***
Отлично (высокий уровень сформированности	*1. Полнота выполнения проекта;* *2. Своевременность*	*Основные требования к выполнения проекта выполнены. Продемонстрировано умение анализировать ситуацию и*

компетенции)	*выполнения;* *3. Правильность ответов на вопросы;* *4. и т.д.*	*находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели*
Хорошо (достаточный уровень сформированности компетенции)		*Основные требования к выполнению проекта 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*
Удовлетворительно (приемлемый уровень сформированности компетенции)		*Имеются существенные отступления от выполнения проекта. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат*
Неудовлетворительно (недостаточный уровень сформированности компетенции)		*Задача выполнения проекта не раскрыта, обнаруживается существенное непонимание проблемы*

Оценивание участников деловой игры

Шкала оценок	***Показатели***	***Критерии***
Отлично (высокий уровень сформированности компетенции)	*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*
Хорошо (достаточный уровень сформированности компетенции)		*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
Удовлетворительно (приемлемый уровень сформированности компетенции)		*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*
Неудовлетворительно (недостаточный уровень сформированности компетенции)		*Задача деловой игры не раскрыта, обнаруживается существенное непонимание проблемы*

Оценивание выполнение лабораторных работ

Шкала оценок	***Показатели***	***Критерии***
Отлично (высокий уровень сформированности компетенции)	1. Полнота выполнения проекта; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. и т.д.	Основные требования к выполнения проекта 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
Хорошо (достаточный уровень сформированности компетенции)		Основные требования к выполнению проекта 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
Удовлетворительно (приемлемый уровень сформированности компетенции)		Имеются существенные отступления от выполнения проекта. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат
Неудовлетворительно (недостаточный уровень сформированности компетенции)		Задача выполнения проекта не раскрыта, обнаруживается существенное непонимание проблемы

Оценивание ответа на экзамене

Шкала оценок	*Показатели*	*Критерии*
Отлично (высокий уровень сформированности компетенции)	1. *Полнота изложения теоретического материала;* 2. *Полнота и правильность решения практического задания;* 3. *Правильность и/или аргументированность изложения (последовательность действий);* 4. *Самостоятельность ответа;* 5. *Культура речи;* 6. *и т.д.*	*Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок.*
Хорошо (достаточный уровень сформированности компетенции)		*Дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.*
Удовлетворительно (приемлемый уровень сформированности компетенции)		*Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.*

Неудовлетворительно (недостаточный уровень сформированности компетенции)		*Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.д студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.*

Лист актуализации оценочных материалов по дисциплине «Комплексная защита объектов информатизации»

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 _____