ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

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

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПО ДИСЦИПЛИНЕ «ЗАЩИТА ИНФОРМАЦИИ ОТ ВНУТРЕННИХ IT-УГРОЗ»

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

Уровень высшего образования – бакалавриат

.

Махачкала – 2023

УДК 681.518(075.8)
ББК 32.81.73

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

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

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

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

Оценочные материалы по дисциплине «Защита информации от внутренних IT-угроз» 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 «Защита информации от внутренних IT-угроз» размещены на официальном сайте www.dgunh.ru

Гасанова З.А. Оценочные материалы по дисциплине «Защита информации от внутренних IT-угроз» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2023 г. – 40 с.

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

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

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

СОДЕРЖАНИЕ

Назначение оценочных материалов

Оценочные материалы разрабатываются для текущего контроля успеваемости (оценивания хода освоения дисциплины), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по дисциплине) обучающихся по дисциплине «Защита информации от внутренних IT-угроз» в целях определения соответствия их учебных достижений поэтапным требованиям образовательной программы высшего образования по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем».

Оценочные материалы по дисциплине «Защита информации от внутренних IT-угроз» 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; контрольные задания или иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине; методические материалы, определяющие процедуры оценивания знаний, умений, навыков, 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, обеспечивающих 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-2.	Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них 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 операционных систем, систем управления базами данных и компьютерных сетей	ИПК-1.1. Администрирует подсистему защиты информации операционных систем	**Знать:** - угрозы безопасности информации и модели нарушителя в операционных системах	Пороговый уровень	Обучающийся слабо (частично) знает угрозы безопасности информации и модели нарушителя в операционных системах	**Блок А** – задания репродуктивного уровня: – вопросы для обсуждения; – тестовые задания.
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает угрозы безопасности информации и модели нарушителя в операционных системах	
			Продвинутый	Обучающийся с требуемой степенью	

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*
			уровень	полноты и точности знает угрозы безопасности информации и модели нарушителя в операционных системах	
		<u>Уметь</u>: - разрабатывать модели угроз и нарушителей информационной безопасности операционных систем	Пороговый уровень	Обучающийся слабо (частично) умеет разрабатывать модели угроз и нарушителей информационной безопасности операционных систем	**Блок В** – задания реконструктивного уровня: – комплект тематик для рефератов.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет разрабатывать модели угроз и нарушителей информационной безопасности операционных систем	
			Продвинутый уровень	Обучающийся умеет разрабатывать модели угроз и нарушителей информационной безопасности операционных систем	
		<u>Владеть</u>: - навыками конфигурирования	Пороговый уровень	Обучающийся слабо (частично) владеет навыками конфигурирования	**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*
		параметров системы защиты операционных систем		параметров системы защиты операционных систем	ориентированного уровня – комплект лабораторных работ.
			Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками конфигурирования параметров системы защиты операционных систем	
			Продвинутый уровень	Обучающийся свободно владеет навыками конфигурирования параметров системы защиты операционных систем	
	ИПК-1.2. Администрирует подсистему защиты информации СУБД	**Знать:** - угрозы безопасности информации и модели нарушителя информационной безопасности СУБД	Пороговый уровень	Обучающийся слабо (частично) знает угрозы безопасности информации и модели нарушителя информационной безопасности СУБД	**Блок А** – задания репродуктивного уровня: – вопросы для обсуждения; – тестовые задания.
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает угрозы безопасности информации и модели нарушителя информационной безопасности СУБД	

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*
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает угрозы безопасности информации и модели нарушителя информационной безопасности СУБД	
		<u>Уметь</u>: - разрабатывать модели угроз и нарушителей информационной безопасности СУБД	Пороговый уровень	Обучающийся слабо (частично) умеет разрабатывать модели угроз и нарушителей информационной безопасности СУБД	**Блок В** – задания реконструктивного уровня – комплект тематик для рефератов.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет разрабатывать модели угроз и нарушителей информационной безопасности СУБД	
			Продвинутый уровень	Обучающийся умеет разрабатывать модели угроз и нарушителей информационной безопасности СУБД	
		<u>Владеть</u>: - навыками конфигурирования параметров системы	Пороговый уровень	Обучающийся слабо (частично) владеет навыками конфигурирования параметров системы защиты информации СУБД	**Блок С** – задания практико-ориентированного уровня

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 СУБД	Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками конфигурирования параметров системы защиты информации СУБД	– комплект лабораторных работ.
			Продвинутый уровень	Обучающийся свободно владеет навыками конфигурирования параметров системы защиты информации СУБД	
	ИПК-1.3. Администрирует подсистему защиты информации компьютерных сетей	**Знать:** - угрозы безопасности информации и модели нарушителя информационной безопасности компьютерных сетей.	Пороговый уровень	Обучающийся слабо (частично) знает угрозы безопасности информации и модели нарушителя информационной безопасности компьютерных сетей	**Блок А –** задания репродуктивного уровня: – вопросы для обсуждения; – тестовые задания.
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает угрозы безопасности информации и модели нарушителя информационной безопасности компьютерных сетей	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает угрозы	

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 информации и модели нарушителя информационной безопасности компьютерных сетей	
		<u>Уметь</u>: - разрабатывать модели угроз и нарушителей информационной безопасности компьютерных сетей.	Пороговый уровень	Обучающийся слабо (частично) умеет разрабатывать модели угроз и нарушителей информационной безопасности компьютерных сетей	**Блок В** – задания реконструктивного уровня: – комплект тематик для рефератов.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет разрабатывать модели угроз и нарушителей информационной безопасности компьютерных сетей	
			Продвинутый уровень	Обучающийся умеет разрабатывать модели угроз и нарушителей информационной безопасности компьютерных сетей	
		<u>Владеть</u>: - навыками конфигурирования параметров системы	Пороговый уровень	Обучающийся слабо (частично) владеет навыками конфигурирования параметров системы защиты информации компьютерных сетей	**Блок С** – задания практико-ориентированного уровня

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 компьютерных сетей	Базовый уровень	Обучающийся с небольшими затруднениями владеет	– комплект лабораторных работ.
			Продвинутый уровень	Обучающийся свободно владеет навыками конфигурирования параметров системы защиты информации компьютерных сетей	
ПК-2. Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	ИПК-2.2. Обеспечивает безопасность информационных технологий, применяемых в автоматизированных системах	**Знать:** - особенности информационных технологий, применяемых в автоматизированных системах	Пороговый уровень	Обучающийся слабо (частично) знает особенности информационных технологий, применяемых в автоматизированных системах	**Блок А –** задания репродуктивного уровня: – вопросы для обсуждения; – тестовые задания.
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает особенности информационных технологий, применяемых в автоматизированных системах	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает особенности информационных технологий, применяемых в	

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*
				автоматизированных системах	
		<u>Уметь</u>: – анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; - осуществлять планирование и организацию работы персонала автоматизиро	Пороговый уровень	Обучающийся слабо (частично) умеет анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации	**Блок В** – задания реконструктивного уровня – комплект тематик для рефератов.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей	

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*
		ванной системы с учетом требований по защите информации		безопасности информации в автоматизированных системах, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации	
			Продвинутый уровень	Обучающийся умеет анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации	
		<u>Владеть</u>:	Пороговый уровень	Обучающийся слабо (частично) владеет навыками	**Блок С** – задания

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 конфигурирования параметров системы защиты информации автоматизированных систем, с учетом применяемых информационных технологий		конфигурирования параметров системы защиты информации автоматизированных систем, с учетом применяемых информационных технологий	практико-ориентированного уровня – комплект лабораторных работ.
			Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками конфигурирования параметров системы защиты информации автоматизированных систем, с учетом применяемых информационных технологий	
			Продвинутый уровень	Обучающийся свободно владеет навыками конфигурирования параметров системы защиты информации автоматизированных систем, с учетом применяемых информационных технологий	

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-1.1. Администрирует подсистему защиты информации операционных систем

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

1. Выберите наиболее подходящее определение информации:
   a. Сведения о лицах, предметах;
   b. Сведения о лицах, предметах, фактах, событиях;
   c. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
   d. Сведения о лицах независимо от формы их представления.
2. Информационная система – это …
   a. Набор программных и технических средств;
   b. Упорядоченную совокупность документов, информационных технологий и программно-аппаратных средств, реализующих информационные процессы;
   c. Упорядоченная совокупность документов, относящихся к определенной области;
   d. Набор программных средств, относящихся к одной задаче.
3. Информационными ресурсами называют:
   a. Документы (массивы документов), существующие в составе информационных систем;
   b. Документы (массивы документов), существующие отдельно или в составе информационных систем;
   c. Документы (массивы документов), существующие отдельно от информационных систем;
   d. Все определения не верны.
4. Информацию по степени доступа разделяют на:
   a. Открытую и ограниченного доступа;
   b. Открытую;
   c. Закрытую;
   d. Тайную и ограниченную.
5. К информации ограниченного доступа относятся:
   a. Государственная тайна;
   b. Конфиденциальная информация;
   c. Персональные данные;
   d. Все ответы верны.

6. Собственник информационных ресурсов, систем и технологий – это:
   a. Субъект с полномочиями владения указанными объектами;
   b. Субъект с полномочиями владения и пользования указанными объектами;
   c. Субъект с полномочиями владения, пользования и распоряжения указанными объектами;
   d. Все ответы верны.
7. Защитой информации называют:
   a. Деятельность по предотвращению утечки любой информации;
   b. Деятельность по предотвращению утечки защищаемой информации;
   c. Деятельность по предотвращению утечки доступной информации;
   d. Все ответы верны.
8. Под утечкой понимают:
   a. Неконтролируемое распространение защищаемой информации путём её разглашения или несанкционированного доступа к ней;
   b. Неконтролируемое распространение скрытой информации путём её разглашения или несанкционированного доступа к ней;
   c. Неконтролируемое распространение конфиденциальной информации путём её разглашения или несанкционированного доступа к ней;
   d. Все верно.
9. Под непреднамеренным воздействием на защищаемую информацию понимают:
   a. Воздействие на неё из-за ошибок пользователя, сбоя технических или программных средств, иных нецеленаправленных действий;
   b. Воздействие на неё из-за ошибок пользователя, сбоя технических средств;
   c. Воздействие на неё из-за ошибок пользователя, программных средств, иных нецеленаправленных действий;
   d. Все ответы верны.
10. Что не относится к задачам информационной безопасности:
   a. Целостность и секретность;
   b. Электронная подпись и датирование;
   c. Устойчивость связи и определение трафика;
   d. Неотказуемость и анонимность.
11. К методам обеспечения информационной безопасности не относятся:
   a. Корпоративные;
   b. Административные;
   c. Правовые;
   d. Технические.
12. Какие методы не относятся к обеспечению информационной безопасности:
   a. Принуждение и побуждение;
   b. Управление доступом и регламентация;
   c. Маскировка и препятствие;
   d. Скрытый доступ и копирование сообщений.
13. Метод физического преграждения пути злоумышленнику к информации:
   a. Управление доступом;

b. Маскировка;
c. Принуждение;
d. Побуждение.

14. Метод защиты информации путем ее криптографического преобразования:
    a. Принуждение;
    b. Побуждение;
    c. Маскировка;
    d. Управление доступом.
15. Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам:
    a. Уполномочивание;
    b. Контроль доступа;
    c. Сертификация;
    d. Нет верного ответа.
16. Основными характеристиками защищаемой информации являются:
    a. Конфиденциальность, целостность и статичность;
    b. Конфиденциальность, целостность и доступность;
    c. Аутентификация, целостность и доступность;
    d. Аутентификация, статичность и время создания.
17. Известность содержания информации только имеющим соответствующие полномочия субъектам – это:
    a. Целостность;
    b. Статичность;
    c. Конфиденциальность;
    d. Аутентификация.
18. Неизменность информации в условиях её случайного и (или) преднамеренного искажения и разрушения – это:
    a. Целостность;
    b. Конфиденциальность;
    c. Доступность;
    d. Идентификация.
19. Возможность получения информации или информационной услуги за приемлемое время – это:
    a. Конфиденциальность;
    b. Целостность;
    c. Доступность;
    d. Статичность.
20. Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:
    a. Уязвимость;
    b. Атака;
    c. Угроза;
    d. Нет верного ответа;

21. Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого её состояния, при котором создаются условия для реализации угроз безопасности информации - это:
    a. Атака;
    b. Угроза;
    c. Уязвимость;
    d. Статичность.
22. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации – это:
    a. Статичность;
    b. Атака;
    c. Угроза;
    d. Изъян.
23. Классификацию угроз ИБ можно выполнить по нескольким критериям:
    a. По аспекту информационной безопасности;
    b. По компонентам информационной системы;
    c. По способу осуществления;
    d. Все ответы верны.
24. Конфиденциальная информация может быть разделена на:
    a. Предметную и служебную;
    b. Служебную и закрытую;
    c. Предметную и открытую;
    d. Открытую и закрытую.
25. Целостность информации может быть разделена на:
    a. Статическую и динамическую;
    b. Статическую и служебную;
    c. Служебную и динамическую;
    d. Все верно.
26. Примером нарушения статической целостности не является:
    a. Ввод неверных данных;
    b. Несанкционированное изменение данных;
    c. Изменение программного модуля вирусом;
    d. Внесение дополнительных пакетов в сетевой трафик.
27. Примером нарушения динамической целостности не является:
    a. Нарушение атомарности транзакций;
    b. Внесение дополнительных пакетов в сетевой трафик;
    c. Несанкционированное изменение данных;
    d. Дублирование данных.
28. Самая распространенная формальная модель доступа к данным:
    a. Мандатная модель;
    b. Дискреционная модель;
    c. Модель Биба;
    d. Модель Кларка.

29. В дискреционной модели отношения субъекты – объекты представлены в виде:
a. Таблиц;
b. Матриц;
c. Схем;
d. Все ответы верно.
30. В какой модели доступа каждому объекту системы присвоена метка секретности?
a. Модель Кларка;
b. Дискреционная модель;
c. Мандатная модель;
d. Модель Биба.
31. Центральный элемент системы защиты, который идентифицирует субъекты, объекты и параметры запрашиваемого доступа субъектов к объектам:
a. Сканер безопасности;
b. Монитор безопасности;
c. Модем безопасности;
d. Шина безопасности.
32. К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые:
a. Руководством организации;
b. Персоналом организации;
c. Пользователями;
d. Нет верного ответа.
33. Наиболее распространёнными методами несанкционированного доступа в операционной системе Windows является:
a. Позволяющие несанкционированно запустить исполняемый код;
b. Позволяющие обойти установленные разграничения прав доступа;
c. Троянские программы;
d. Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов.
34. Что не относится к недостаткам ОС Windows?
a. Невозможно встроенными средствами гарантированно удалять остаточную информацию;
b. Не обеспечивается регистрация выдачи документов на "твёрдую копию", а также некоторые другие требования к регистрации событий;
c. Невозможно в общем случае обеспечить замкнутость (или целостность) программной среды;
d. Невозможно встроенными средствами обеспечить полноту системы.

А2. Вопросы для обсуждения

1. Что такое защита информации? Цель защиты информации.
2. Характеристики информации, относящиеся к задачам защиты.
3. Меры по защите информационной системы.

4. Основные задачи информационной безопасности.
5. Основные методы по защите информационной системы.
6. Модели разграничения доступа
7. Угрозы безопасности операционных систем

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов

1. Программы для восстановления информации на жестких дисках.
2. Сравнительный анализ уязвимостей операционных систем.
3. Программное обеспечение для резервного копирования информации.

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

С1. Лабораторные работы

Лабораторная работа №1. Методика устранения компьютерной информации.

Цель работы: Приобретение навыков устранения и восстановления информации на различных носителях.

Задачи:

1. Физическая организация жестких дисков.
2. Методы восстановления информации.
3. Обзор современных средств устранения компьютерной информации.

Лабораторная работа №2. Уязвимости операционных систем семейства Windows.

Цель работы: Приобретение навыков настройки Windows для уменьшения уязвимостей.

Задачи:

1.Недостатки архитектуры операционных систем семейства Windows .

2.Основные виды уязвимостей: статистика их обнаружения и устранения.

3.Описание методик атак, использующих уязвимости операционной системы семейства Windows.

4.Настройка операционной системы для увеличения обороноспособности вычислительной системы.

Лабораторная работа №3. Защита от копирования переносных носителей.

Цель работы: Приобретение навыков защиты от копирования переносных носителей.

Задачи:

1. Методика защиты программных и установочных дисков.
2. Методика защиты дисков с данными.
3. Современные средства защиты видеодисков.

Лабораторная работа №4. Аппаратные ключи защиты.

Цель работы: Приобретение навыков защиты данных с помощью аппаратных ключей.

Задачи:

1. Основные виды аппаратных ключей.
2. Методики обхода аппаратных ключей.
3. Недостатки аппаратных ключей.

Блок D. Задания для использования в рамках промежуточной аттестации

D1. Перечень вопросов к экзамену

1. Выбор направления защиты и методов обеспечения информационной безопасности при защите от внутренних IT-угроз.
2. Источники внутренних IT-угроз.
3. Классификация внутренних IT-угроз.
4. Программно-аппаратные методы защиты от внутренних IT-угроз.
5. Подсистемы защиты информации операционных систем

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-1.2. Администрирует подсистему защиты информации СУБД

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

1. Назовите методы подбора паролей пользователей:
   а) Тотальный перебор
   б) Тотальный перебор, оптимизированный по статистике встречаемости символов
   в) Тотальный перебор, оптимизированный с помощью словарей
   г) Подбор пароля с использованием знаний о пользователе
   д) верны все варианты

2. Какая из ниже представленных моделей относится к модели разграничения доступа к данным?
   а) Мандатная;
   б) модель Биба;
   в) модель Кларка;

г) нет верного ответа.

3. Какая из ниже представленных моделей относится к модели разграничения доступа к данным?

а) Дискреционная;
б) модель Биба;
в) модель Кларка;
г) нет верного ответа.

4. В дискреционной модели отношения субъекты - объекты представлены в виде:

а) Таблиц;
б) Матриц;
в) Схем;
г) все верно;

5. В какой модели доступа каждому объекту системы присвоена метка секретности:

а) модель Кларка;
б) дискреционная;
в) мандатная;
г) модель Биба

6. Какая из ниже представленных команд создает пользователя?

а) CREATE USER,
б) CREATE VIEW,
в) CREATE SYNONYM
г) CREATE ROLE

7. Какая команда используется для назначения привилегий пользователям?

а) GRANT
б) SET ROLE
в) SET TRANSACTION
г) REVOKE

8. Какая команда используется для отмены привилегий, назначенных пользователю?

а) GRANT
б) SET ROLE
в) SET TRANSACTION
а) REVOKE

9. В какой системе, строится модель избирательного управления доступом к данным:

а) модель Кларка;

б) дискреционная;
в) мандатная;
г) модель Биба

10. Реляционная база данных - это?
а) БД, в которой информация организована в виде прямоугольных таблиц;
б) БД, в которой элементы в записи упорядочены, т.е. один элемент считается главным, остальные подчиненными;
в) БД, в которой записи расположены в произвольном порядке;
г) БД, в которой принята свободная связь между элементами разных уровней.

А2. Вопросы для обсуждения

1. Репликация транзакций. Репликация сведением.
2. Управление транзакциями, сериализация транзакций. Транзакции и целостность баз данных. Изолированность пользователей.
3. Сериализация транзакций. Методы сериализации транзакций.
4. Синхронизационные захваты. Гранулированные синхронизационные захваты. Предикатные синхронизационные захваты.
5. Тупики, распознавание и разрушение. Метод временных меток.
6. Журнализация изменений БД. Журнализация и буферизация. Индивидуальный откат транзакции.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов

1. Средства и методы защиты информации при использовании СУБД RBase
2. Средства и методы защиты информации при использовании СУБД Dbase
3. Средства и методы защиты информации при использовании СУБД FoxBase
4. Средства и методы защиты информации при использовании СУБД FoxPro
5. Средства и методы защиты информации при использовании СУБД Paradox
6. Средства и методы защиты информации при использовании СУБД Oracle
7. Средства и методы защиты информации при использовании СУБД Cache
8. Средства и методы защиты информации при использовании технологии Com

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

С1. Лабораторные работы

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.

Блок D. Задания для использования в рамках промежуточной аттестации

D1. Перечень вопросов к экзамену

1. Аксиома безопасности базы данных. Примеры.
2. SQL-инъекции, свойства, методы противодействия.
3. Автоматизированные средства защиты от SQL-инъекции. Сильные и слабые стороны Web Application Firewall и экранирование.
4. Угрозы, специфичные для СУБД.
5. Метки безопасности и принудительный контроль доступа.
6. Поддержание целостности данных. Табличные, ссылочные ограничения. Правила.
7. Методы обеспечения доступности баз данных. Информационная избыточность.
8. Методы обеспечения доступности баз данных. Аппаратная избыточность.
9. Методы обеспечение конфиденциальности данных. Криптографические методы в СУБД.
10. Методы обеспечения конфиденциальности данных. Внедрение sql-кода.

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-1.3. Администрирует подсистему защиты информации компьютерных сетей

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

1. Угроза отказа служб может быть разбита на следующие типы:
   a. Отказ пользователей;
   b. Внутренний отказ информационной системы;
   c. Отказ поддерживающей инфраструктуры;
   d. Все ответы верны.
2. Что не относится к внутреннему отказу ИС?
   a. Ошибки при переконфигурировании системы;

b. Отказы программного и аппаратного обеспечения;
c. Разрушение данных;
d. Нарушение работы систем связи.

3. Что не относится к отказу служб?
   a. Нарушение работы систем связи;
   b. Разрушение и повреждение помещений;
   c. Нарушение работы электропитания;
   d. Разрушение данных.
4. Какая угроза отказа служб устраняется административно-правовыми методами?
   a. Отказ пользователей;
   b. Отказ программного обеспечения;
   c. Нарушение работ систем связи;
   d. Разрушение и повреждение помещений.
5. К каналам, предполагающим изменение элементов информационной структуры относится:
   a. Намеренное копирование файлов и носителей информации;
   b. Маскировка под других пользователей, путём похищение идентифицирующей их информации;
   c. Хищение носителей информации;
   d. Незаконное подключение специальной регистрирующей аппаратуры к устройствам связи.
6. Что относится к каналам, не требующим изменение элементов ИС?
   a. Намеренное копирование файлов и носителей информации;
   b. Незаконное подключение специальной регистрирующей аппаратуры;
   c. Злоумышленное изменение программ;
   d. Злоумышленный вывод из строя средств защиты информации.
7. Какая направленность атак неверно сформулирована?
   a. Атаки на уровне операционной системы;
   b. Атаки на уровне системного администратора;
   c. Атаки на уровне сетевого программного обеспечения;
   d. Атаки на уровне систем управления базами данных.
8. К какому типу атак относится прослушивание передаваемых сообщений?
   a. Пассивная атака;
   b. Модификация потока данных;
   c. Повторное использование;
   d. Отказ в обслуживании.

А2. Вопросы для обсуждения

1. Классификация угроз информационной безопасности.
2. Классификация нарушителей.
3. Утечка информации, каналы утечки информации и их характеристики.
4. Классификация угроз в сетях передачи данных
5. Особенности защиты распределенных систем

6. Политика безопасности на предприятии.
7. Уровни правового обеспечения информационной безопасности.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов

1. Формирование политики безопасности с учетом актуальных угроз.
2. Организация защиты от несанкционированного доступа.
3. Системы обнаружения атак
4. Анализаторы защищенности сетей

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

С1. Лабораторные работы.

Лабораторная работа «Защита ЛВС от атак канального уровня».

Целью лабораторной работы является изучение методов проектирования, развертывания и настройки механизмов защиты в коммутируемых ЛВС от атак канального уровня типа MAC-flooding и MAC-spoofing.

Постановка задачи: В сегменте ЛВС филиала, построенном на базе двух коммутаторов уровня доступа Cisco Catalyst 2960 и коммутатора уровня ядра-распределения Cisco Catalyst 3560, обеспечить защиту от атак типа MAC-flooding и MAC-spoofing.

Последовательность действий:

Шаг 1. На коммутаторе уровня доступа SW4-3 настроить механизм port security в динамическом режиме для рабочих станций:

```
interface range fa0/2-3
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security violation protect
```

Шаг 2. Выполнить аналогичные настройки механизма port security на коммутаторе SW4-2.

Шаг 3. На коммутаторе уровня ядра-распределения SW4-1 настроить механизм port security в статическом режиме с привязкой к заданному MAC-адресу для порта FastEthernet0/4:

```
interface fa0/4
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address xxxx.yyyy.zzzz
switchport port-security violation shutdown
```

Шаг 4. На коммутаторе уровня ядра-распределения SW4-1 настроить механизм port security в статическом режиме с опцией sticky для порта FastEthernet0/5:

interface fa0/5
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown

Шаг 5. Проверить корректность настроек механизма безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-spoofing. Задать MAC-адрес рабочей станции, подключенной к порту коммутатора со статическим методом формирования списка MAC-адресов, несоответствующий требованиям политики безопасности. Убедиться в переводе порта коммутатора в режим shutdown или protect.

Шаг 6. Проверить корректность настроек механизма безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-flooding. На порт коммутатора с динамическим методом формирования списка разрешенных MAC-адресов подключить коммутатор с несколькими рабочими станциями. Убедиться в переводе порта коммутатора в режим shutdown или protect.

Блок D. Задания для использования в рамках промежуточной аттестации

D1. Перечень вопросов к экзамену

1. Виды технической документации на информационные системы.
2. Правовые методы защиты от внутренних IT-угроз.
3. Организационные методы защиты от внутренних IT-угроз.
4. Классификация внутренних нарушителей.

Для проверки сформированности компетенции ПК-2. Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации
ИПК-2.2. Обеспечивает безопасность информационных технологий, применяемых в автоматизированных системах

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

1. Возможность изменения применяемых средств ИС – это:
   a. Комплексность;
   b. Гибкость;
   c. Непрерывность;
   d. Целостность.

2. Политика безопасности верхнего уровня, затрагивающая все организацию в целом, включает в себя:
   a. Решение сформировать или изменить комплексную программу обеспечения информационной безопасности;
   b. Формулирование целей организации в области информационной безопасности, определение общих направлений в достижении данных целей;
   c. Обеспечение нормативной базы для соблюдения законов и правил;
   d. Все ответы верны.
3. Что из перечисленного не входит в первый уровень правового обеспечения информационной безопасности?
   a. Конституция РФ (ст. 23, право на тайну переписки);
   b. Гражданский кодекс РФ (ст. 139, возмещение убытков от утечек);
   c. Федеральный закон "О государственной тайне";
   d. Постановления Правительства РФ.
4. Что из перечисленного не входит во второй уровень правового обеспечения информационной безопасности?
   a. Указы Президента РФ;
   b. Постановления Правительства РФ;
   c. Уголовный кодекс РФ (ст. 272-274, неправомерный доступ, распространение вирусов, нарушение правил эксплуатации);
   d. Постановления пленумов Верховного Суда РФ.
5. Систему национальной безопасности образует:
   a. Органы законодательной, исполнительной и судебной властей;
   b. Государственные, общественные и иные организации и объединения;
   c. Граждане, принимающие участие в обеспечении безопасности в соответствии с законом;
   d. Все ответы верны.
6. Что не относится к основным принципам обеспечения национальной безопасности?
   a. Законность;
   b. Соблюдение баланса жизненно важных интересов личности, общества и государства;
   c. Взаимная ответственность личности, общества и государства по обеспечению безопасности;
   d. Системность.
7. К правовым методам обеспечения информационной безопасности относят:
   a. Разработка современных методов и средств защиты информации;
   b. Определение ответственности физических и юридических лиц;
   c. Усиление контроля за развитием информационного рынка России;
   d. Повышение степени защищенности законных интересов граждан.
8. Когда был принят Федеральный закон «Об информации, информатизации и защите информации»?
   a. 2004;
   b. 2006;

c. 2008;
d. 2010.

9. Что не относится к основным аппаратным средствам защиты информации:
   a. Пластиковые карты;
   b. Электронные замки;
   c. Магнитные карты;
   d. Видео карты.
10. Какой из перечисленных уровней предусматривает логическую защиту информации?
   a. Внешний уровень, охватывающий всю территорию расположения вычислительной системы;
   b. Уровень отдельных сооружений или помещений;
   c. Уровень технологических процессов хранения, обработки и передачи информации;
   d. Уровень компонентов вычислительной системы.
11. Какой из перечисленных классов не относится к классам защиты информации?
   a. Физический;
   b. Программно-аппаратный;
   c. Технологический;
   d. Организационный.
12. Какие из перечисленных средств применяются для физической защиты информации?
   a. Лазерные и оптические системы;
   b. Механические и электронные замки;
   c. Телевизионные системы наблюдения;
   d. Все ответы верные.
13. Для регистрации событий подключения к ВС ведется:
   a. Видеонаблюдение;
   b. База данных;
   c. Аудит;
   d. Протокол.
14. Защита от несанкционированного доступа со стороны пользователей в современных системах в основном реализуется:
   a. Парольная защита;
   b. Аутентификация;
   c. Идентификация;
   d. Все ответы верные.
15. Какой из перечисленных способов не используется для аутентификации пользователя?
   a. Запрос секретного пароля;
   b. Применение микропроцессорных карточек;
   c. Биометрические средства;
   d. Датирование.

16. Сложный вариант электронного ключа – это:
    a. Пластиковая карта;
    b. Электронный жетон;
    c. Криптографический шифр;
    d. Электронная цифровая подпись.
17. Из множества существующих средств аутентификации, наиболее надежными являются:
    a. Средства распознавания;
    b. Биометрические средства;
    c. Электронный ключ;
    d. Микропроцессорные карточки.
18. Что не относится к биометрическим средствам:
    a. Отпечаток пальца;
    b. Сетчатка глаза;
    c. Голос;
    d. Имя.
19. Сбор и накопление информации о событиях информационной системы – это:
    a. Протоколирование;
    b. Аудит;
    c. Журнал данных;
    d. Синтез.
20. Анализ накопленной информации, проводимый оперативно или периодически:
    a. Синтез;
    b. Протоколирование;
    c. Аудит;
    d. Нет правильного варианта.
21. При протоколировании рекомендуют записывать следующую информацию:
    a. Дата и время события;
    b. Результат события;
    c. Источник запроса;
    d. Все ответы верные.
22. Исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения:
    a. Паразит;
    b. Вирус;
    c. Призрак;
    d. Нет верного ответа.
23. По особенностям реализуемого алгоритма вирусы делятся на:
    a. Спутники, стелсы, паразиты, призраки;
    b. Стелсы, спутники, призраки, черви;
    c. Паразиты, призраки, черви, стелсы;
    d. Нет верного ответа.
24. Что необходимо иметь для проверки на наличие вирусов на жестком диске?
    a. Защищенную программу;

b. Загрузочную программу;
c. Файл с сигнатурами вирусов;
d. Антивирусную программу.

25. Основными путями проникновения вирусов в компьютер являются:
a. Внешние носители информации;
b. Компьютерные сети;
c. Действия пользователя;
d. Все ответы верные.

26. Компьютерные вирусы:
a. Возникают в связи со сбоями в аппаратных средствах компьютера;
b. Пишутся людьми специально для нанесения ущерба;
c. Зарождаются при работе неверно написанных программных продуктов;
d. Являются следствием ошибок в операционной системе.

27. Загрузочные вирусы характеризуются тем, что:
a. Поражают загрузочные сектора дисков;
b. Поражают программы в начале их работы;
c. Запускаются при загрузке компьютера;
d. Изменяют весь код заражаемого файла.

28. Вирус, у которого каждая следующая копия в заражённых объектах отличается от предыдущих – это:
a. Стелс;
b. Спутник;
c. Призрак;
d. Паразит.

A2. Вопросы для обсуждения

1. Сервисы безопасности.
2. Методы идентификации и аутентификации.
3. Протоколирование действий пользователей и аудит безопасности.
4. Виды технических каналов утечки информации.
5. Каналы утечки информации при её передаче по каналам связи.

Блок B. Задания реконструктивного уровня («уметь»)

B1. Тематика рефератов

1. Организационные методы противодействия внутренним нарушителям.
2. Технические средства защиты информации.
3. Разграничение доступа к информационным ресурсам.
4. Программно-аппаратные средства разграничения доступа.
5. Программно-аппаратные средства администрирования информационных ресурсов.

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

С2. Лабораторные работы

Лабораторная работа №1. Антивирусное программное обеспечение.

Цель работы: Приобретение навыков защиты информации используя антивирусное программное обеспечение.

Задачи:

1. Программы-шпионы. Защита от программ шпионов.
2. Троянские программы.
3. "Черви", методики проникновения.
4. Вирусы, алгоритмы работы.
5. Антивирусное программное обеспечение: рекомендуемые настройки, правила использования.

Блок D. Задания для использования в рамках промежуточной аттестации

D1. Перечень вопросов к экзамену

1. Общая постановка задачи защиты от внутренних IT-угроз.
2. Виды конфиденциальной информации и уровни защиты.
3. Администрирование информационных ресурсов организации.
4. Администрирование информационных потоков организации.

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

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

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

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

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

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

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

Уровни освоения компетенций	Продвинутый уровень	Базовый уровень	Пороговый уровень	Допороговый уровень
100 – балльная шкала	85 и ≥	70 – 84	51 – 69	0 – 50
4 – балльная шкала	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»

Шкала оценок при текущем контроле успеваемости по различным показателям

Показатели оценивания сформированности компетенций	***Баллы***	***Оценка***
Выполнение лабораторных работ	0-20	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Устный опрос	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение и публичная защиты реферата	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	0-20	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по текущему контролю успеваемости

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-50	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины
51-69	«удовлетворительно»	Пороговый уровень	Не менее 50% заданий, подлежащих текущему контролю успеваемости,

			выполнены без существенных ошибок
70-84	«хорошо»	Базовый уровень	Обучающимся выполнено не менее 75% заданий, подлежащих текущему контролю успеваемости, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала и применения его при решении практических заданий; задания выполнены без ошибок
85-100	«отлично»	Продвинутый уровень	100% заданий, подлежащих текущему контролю успеваемости, выполнены самостоятельно и в требуемом объеме; обучающийся проявляет умение обобщать, систематизировать материал и применять его при решении практических заданий; задания выполнены с подробными пояснениями и аргументированными выводами

Шкала оценок по промежуточной аттестации

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

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

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

	льно»	уровень	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, характеризующих этапы формирования компетенций

Устный опрос проводится в первые 15 минут занятий семинарского типа в формате обсуждения с названными преподавателем студентами. Остальные обучающиеся вправе дополнить или уточнить ответ по своему желанию (соблюдаю очередность ответа). Основной темой для опроса являются вопросы для обсуждения, соответствующие теме предыдущей лекции, но преподаватель может уточнять задаваемый вопрос, задавать наводящие вопросы или сужать вопрос до отдельного аспекта обсуждаемой темы.

Методика оценивания ответов на устные вопросы

Баллы	***Оценка***	***Показатели***	***Критерии***
9-10	«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.
7-8	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
5-6	«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.
0-4	«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**
18-20	«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
14-17	«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.
11-13	«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.
0-10	«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***
9-10	«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.
7-8	«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.
5-6	«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.

0-4	«неудовле твори-тельно»		Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы, не проведена защита реферата.

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»	1. Полнота выполнения задания лабораторной работы; 2. Своевременность выполнения задания лабораторной работы; 3. 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-тельно»		Шаги выполнения лабораторной работы не выполнены, обнаруживается существенное непонимание проблемы.

В экзаменационный билет включено два теоретических вопроса. Экзамен проводится в виде письменного ответа на вопрос билета. При оценке ответа на вопрос оценивается полнота ответа, точность формулировок, правильное цитирование соответствующих законодательных актов, наличие иллюстративных примеров. Время подготовки ответа при сдаче экзамена составлять 60 минут.

Оценка ответов, подготовленных студентами объявляется обучающимся в день проведения экзамена.

Методика оценивания ответа на экзамене

Баллы	Оценка	Показатели	Критерии
18-20	«отлично»	1. Полнота и последовательность ответа на поставленные вопросы; 2. Логичность и аргументированность изложения; 3. Наличие практических примеров.	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 и систематизировать материал.
14-17	«хорошо»		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 примера-ми; обучающийся показал хорошие знания по предмету, владение навыками систематизации материала.
11-13	«удовлетворительно»		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.
0-10	«не удовлетворительно»		Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы.

Лист актуализации оценочных материалов по дисциплине
«Защита информации от внутренних IT-угроз»

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 _____