Приложение А

(обязательное к рабочей программе дисциплины)

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Информационная безопасность открытых систем»

Уровень образования — **специалитет** (бакалавриат/магистратура/специалитет)

Специальность — **10.05.03 Информационная безопасность автоматизированных систем** (код, наименование специальности)

Специализация — **Безопасность открытых информационных систем** (наименование)

Разработчик _____ (подпись) Качаева Г.И. (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБ «20» сентября 2021г., протокол № 2

Зав. кафедрой _____ (подпись) Качаева Г.И. (ФИО уч. степень, уч. звание)

г. Махачкала 2021

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Информационная безопасность открытых систем» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. по самостоятельной работе студентов, далее – СРС), освоивших программу данной дисциплины.

Целью фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Рабочей программой дисциплины «Информационная безопасность открытых систем» предусмотрено формирование следующих компетенций:

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;

ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем;

ОПК-5.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах.

Код компетенции	**Наименование компетенции**	**Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)**
ОПК-4	Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.2.6 умеет осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий
ОПК-5.2	Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ОПК-5.2.1.1 знает методы и средства обеспечения информационной безопасности открытых информационных систем;
		ОПК-5.2.1.2 знает методы контроля, разработки эксплуатационной документации, обслуживания систем защиты информации открытых информационных систем;
		ОПК-5.2.2.1 умеет применять методы и средства защиты информации открытых информационных систем;
		ОПК-5.2.2.2 умеет разрабатывать эксплуатационную документацию, требования по эксплуатации систем защиты открытых информационных систем;
ОПК-5.3	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ОПК-5.3.1.1 знает основные информационные технологии, используемые в автоматизированных системах;
		ОПК-5.3.1.2 знает системы управления информационной безопасностью

		открытой информационной системы;
		ОПК-5.3.2.1 умеет работать с интегрированной средой разработки программного обеспечения;
		ОПК-5.3.2.2 умеет анализировать представленную в общедоступных источниках информацию о современных тенденциях в области информационных систем;

2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)

Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля), и используемые оценочные средства приведены в таблице 1.

Перечень оценочных средств, рекомендуемых для заполнения таблицы 1 (в ФОС не приводится, используется только для заполнения таблицы)

- *Устный опрос*
- *Вопросы для проведения экзамена*

2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП

Таблица 1

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Критерии оценивания	Наименование контролируемых разделов и тем1
ОПК-4 -Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.2.6 умеет осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий	Знать: Основные угрозы безопасности информации и модели нарушителя в информационных (автоматизированных) систем; Уметь: Анализировать и оценивать угрозы информационной безопасности объекта	№№ 1-34
ОПК-5.2 - Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ОПК-5.2.1.1 знает методы и средства обеспечения информационной безопасности открытых информационных систем; ОПК-5.2.1.2 знает методы контроля, разработки эксплуатационной документации, обслуживания систем защиты информации открытых информационных систем; ОПК-5.2.2.1 умеет применять методы и средства защиты информации	Знать: методы и средства обеспечения информационной безопасности открытых информационных систем; методы контроля, разработки эксплуатационной документации, обслуживания систем защиты информации открытых информационных систем; Уметь: применять методы и средства защиты информации открытых информационных систем; разрабатывать эксплуатационную документацию, требования по эксплуатации систем защиты открытых информационных систем;	№№ 1-34

[1] *Наименования разделов и тем должен соответствовать рабочей программе дисциплины.*

	открытых информационных систем;		
	ОПК-5.2.2.2 умеет разрабатывать эксплуатационную документацию, требования по эксплуатации систем защиты открытых информационных систем;		
ОПК-5.3 -Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ОПК-5.3.1.1 знает основные информационные технологии, используемые в автоматизированных системах;	Знать: основные информационные технологии, используемые в автоматизированных системах; системы управления информационной безопасностью открытой информационной системы; Уметь: работать с интегрированной средой разработки программного обеспечения; анализировать представленную в общедоступных источниках информацию о современных тенденциях в области информационных систем;	№№ 1-34
	ОПК-5.3.1.2 знает системы управления информационной безопасностью открытой информационной системы;		
	ОПК-5.3.2.1 умеет работать с интегрированной средой разработки программного обеспечения;		
	ОПК-5.3.2.2 умеет анализировать представленную в общедоступных источниках информацию о		
	современных тенденциях в области информационных систем;		

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Информационная безопасность открытых систем определяется на следующих этапах:

1. **Этап текущих аттестаций** *(Для проведения текущих аттестаций могут быть использованы оценочные средства, указанные в разделе 2*)

2. **Этап промежуточных аттестаций** (*Для проведения промежуточной аттестации могут быть использованы другие оценочные средства*)

Таблица 2

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	**Этапы формирования компетенции**					
		Этап текущих аттестаций					**Этап промежуточной аттестации**
		1-5 неделя	**6-10 неделя**	**11-15 неделя**	**1-17 неделя**		**18-20 неделя**
		Текущая аттестация №1	Текущая аттестация №2	Текущая аттестация №3	СРС	КР/КП	Промежуточная аттестация
1		**2**	**3**	**4**	**5**	**6**	**7**
ОПК-4 -Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.2.6 умеет осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
ОПК-5.2 - Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ОПК-5.2.1.1 знает методы и средства обеспечения информационной безопасности открытых информационных систем;	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-5.2.1.2 знает методы контроля, разработки эксплуатационной документации, обслуживания систем защиты информации						

	открытых информационных систем;						
	ОПК-5.2.2.1 умеет применять методы и средства защиты информации открытых информационных систем;						
	ОПК-5.2.2.2 умеет разрабатывать эксплуатационную документацию, требования по эксплуатации систем защиты открытых информационных систем;						
ОПК-5.3 -Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ОПК-5.3.1.1 знает основные информационные технологии, используемые в автоматизированных системах;	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-5.3.1.2 знает системы управления информационной безопасностью открытой информационной системы;						
	ОПК-5.3.2.1 умеет работать с интегрированной средой разработки программного обеспечения;						
	ОПК-5.3.2.2 умеет анализировать представленную в общедоступных						

	источниках информацию о современных тенденциях в области информационных систем;						

СРС – самостоятельная работа студентов;
КР – курсовая работа;
КП – курсовой проект.

2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания

2.2.1. Показатели уровней сформированности компетенций на этапах их формирования

Результатом освоения дисциплины Информационная безопасность открытых систем является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

Таблица 3

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Высокий (оценка «отлично», «зачтено»)	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Повышенный (оценка «хорошо», «зачтено»)	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные.

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков
Базовый (оценка «удовлетворительно», «зачтено»)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач
Низкий (оценка «неудовлетворительно», «не зачтено»)	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков	

Показатели уровней сформированности компетенций могут быть изменены, дополнены и адаптированы к конкретной рабочей программе дисциплины.

2.2.2. Описание шкал оценивания

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			Критерии оценивания
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП

3.1. Задания и вопросы для входного контроля

1. Архитектура безопасности ИТС .Источники и последствия реализации угроз ИБ
2. Функция, способы и средства обеспечения ИБ
3. Архитектура безопасности ЭМВОС.
4. Принципы архитектуры безопасности сети Интернет
5. Сетевой сегмент безопасности
6. Общая информация для обеспечения безопасности. Метки безопасности.
7. Криптографические проверочные суммы . Сертификаты безопасности
8. Способы защиты сертификатов безопасности. Маркеры безопасности.
9. Общие средства обеспечения безопасности: вспомогательные и функциональные средства
10. Взаимосвязи между способами защиты информации.

3.2. Оценочные средства и критерии сформированности компетенций

Комплект заданий для контрольной работы №1 для первой аттестации

Время выполнения __90_ мин

1. Отказ в обслуживании и доступность.
2. Теоретические основы аутентификации. Общие положения
3. Основные концепции аутентификаци
4. Практические аспекты функционирования С Л А У
5. Принципы, используемые при аутентификации.
6. Фазы (этапы) аутентификации
7. Типы участников информационного взаимодействия
8. Аутентификация физического лица (гражданина, пользователя), или персонификация. Типы атак на процедуру аутентификации
9. Средства аутентификации.
10. Свойства способов аутентификации. Симметричные/асимметричные методы аутентификации.
11. Использование криптографических/ некриптографических методов аутентификации.
12. Типы аутентификации
13. Способы аутентификации. Классификация по критерию уязвимости
14. Характеристики классов способов аутентификации
15. Аутентификация . Классификация на основе конфигурации
16. Аутентификация. Взаимодействие служб и способов обеспечения безопасности с: управлением доступом, целостностью данных, конфиденциальностью данных, неотказуемостью, аудитом
17. Персонификация (аутентификация пользователей). Общие положения
18. Аутентификация в ЭМВОС и Интернет-архитектуре . Аутентификация объекта.
19. Аутентификация источника данных. Использование аутентификации уровнями ЭМВОС и Интернет-архитектуры.
20. Защита процедуры аутентификации. Атаки типа «прослушивание/повторная передача». Атаки типа «повторная передача одной и той же проверяющей стороне»
21. Аутентификация. Атаки типа «повторная передача разным проверяющим сторонам». Атаки типа «перехват/повторная передача».

22. Теоретические основы управления доступом. Общие положения. Цель управления доступом
23. Основные аспекты управления доступом. Распределение компонентов управления доступом. Распределение компонентов управления доступом в нескольких ССБ.
24. Угрозы управления доступом. Политики управления доступом
25. Отображение политики УД. Управление политиками. Детализация и локализация. Унаследованные правила

Комплект заданий для контрольной работы №2 для второй аттестации

Время выполнения __90_ мин

1. Приоритет среди правил ПЛУД. Правила ПЛУД в режиме «по умолчанию». Отображение политики среди взаимодействующих ССБ.
2. Классификация способов управления доступом
3. Схема управления доступом на основе списков доступа
4. Мандатная схема управления доступом
5. Схема управления доступом на основе меток безопасности
6. Контекстная схема управления доступом
7. Взаимодействие управления доступом с другими СЛБ и СПБ: аутентификации, обеспечения целостности данных, обеспечения конфиденциальности данных, аудит.
8. Управление доступом в ЭМВОС и Интернет-архитектуре.
9. Использование управления доступом в рамках уровней ЭМВОС и Интернет-архитектуры.
10. Распределение компонентов управления доступом . . Реализационные аспекты. Размещение ФПРИ- и ФПРР-модулей
11. Теоретические основы обеспечения неотказуемости. Общие положения. Основные концепции обеспечения неотказуемости
12. Фазы процедуры обеспечения неотказуемости
13. Политики обеспечения неотказуемости
14. Средства обеспечения неотказуемости .
15. Способы обеспечения неотказуемости. .
16. Службы обеспечения неотказуемости, использующая маркеры безопасности (защитные конверты) ДТС .
17. Служба обеспечения неотказуемости, использующие маркеры безопасности и модули, защищающие от несанкционированного вмешательства.
18. Служба обеспечения неотказуемости, использующая ЭЦП
19. Служба обеспечения неотказуемости, использующие метки времени. СЛНТ, промежуточную доверенную третью сторону. СЛНТ, использующая нотариальное заверение.
20. Угрозы служб обеспечения неотказуемости.
21. Службы обеспечения неотказуемости в системах ЭМВОС и Интернет-архитектуры. Служба обеспечения неотказуемости с подтверждением источника данных. Служба обеспечения неотказуемости с подтверждением доставки данных
22. СЛНТ в системах хранения и ретрансляции
23. Восстановление в службе обеспечения неотказуемости. Взаимодействие со службой единого каталога.

Комплект заданий для контрольной работы №3 для второй аттестации

Время выполнения __90_ мин

1. Теоретические основы обеспечения конфиденциальности. Общие положения. Основные концепции обеспечения конфиденциальности.
2. Классы служб обеспечения конфиденциальности.
3. Типы способов обеспечения конфиденциальности

4. Угрозы конфиденциальности
5. Типы атак на конфиденциальность.
6. Политики обеспечения конфиденциальности
7. Отображение (описание) политики конфиденциальности
8. Вспомогательная информация и средства обеспечения конфиденциальности.
9. Способы обеспечения конфиденциальности. Обеспечение конфиденциальности на основе предотвращения доступа.
10. Обеспечение конфиденциальности на основе шифрования.
11. Обеспечение конфиденциальности на основе контекстно-зависимого размещения.
12. Обеспечение конфиденциальности в ЭМВОС и Интернет-архитектуре.
13. Теоретические основы обеспечения целостности. Общие положения. Основные концепции обеспечения целостности
14. Типы служб обеспечения целостности
15. Типы способов обеспечения целостности
16. Угрозы целостности.
17. Типы атак на целостность
18. Политики обеспечения целостности. Описание политики.
19. Вспомогательная информация и средства обеспечения целостности. ВИ, необходимая для обеспечения целостности. Средства обеспечения целостности.
20. Классификация способов обеспечения целостности. Обеспечение целостности на основе криптографии.
21. Обеспечение целостности на основе контекста сообщения.
22. Обеспечение целостности на основе обнаружения нарушений и передачи ответных квитанций.
23. Обеспечение целостности путем препятствования (предотвращения)
24. Обеспечение целостности в ЭМВОС и Интернет-архитектуре. Целостность соединения с восстановлением. Целостность соединения без восстановления. Целостность отдельных полей при виртуальном соединении
25. Целостность внешних данных

3.3. Задания для промежуточной аттестации (экзамена)

Список вопросов к экзамену

1. Архитектура безопасности ИТС .Источники и последствия реализации угроз ИБ
2. Функция, способы и средства обеспечения ИБ
3. Архитектура безопасности ЭМВОС.
4. Принципы архитектуры безопасности сети Интернет
5. Сетевой сегмент безопасности
6. Общая информация для обеспечения безопасности. Метки безопасности.
7. Криптографические проверочные суммы . Сертификаты безопасности
8. Способы защиты сертификатов безопасности. Маркеры безопасности.
9. Общие средства обеспечения безопасности: вспомогательные и функциональные средства
10. Взаимосвязи между способами защиты информации.
11. Отказ в обслуживании и доступность.
12. Теоретические основы аутентификации. Общие положения
13. Основные концепции аутентификаци
14. Практические аспекты функционирования С Л А У
15. Принципы, используемые при аутентификации.
16. Фазы (этапы) аутентификации
17. Типы участников информационного взаимодействия
18. Аутентификация физического лица (гражданина, пользователя), или персонификация.

Типы атак на процедуру аутентификации

19. Средства аутентификации.
20. Свойства способов аутентификации. Симметричные/асимметричные методы аутентификации.
21. Использование криптографических/ некриптографических методов аутентификации.
22. Типы аутентификации
23. Способы аутентификации. Классификация по критерию уязвимости
24. Характеристики классов способов аутентификации
25. Аутентификация . Классификация на основе конфигурации
26. Аутентификация. Взаимодействие служб и способов обеспечения безопасности с: управлением доступом, целостностью данных, конфиденциальностью данных, неотказуемостью, аудитом
27. Персонификация (аутентификация пользователей). Общие положения
28. Аутентификация в ЭМВОС и Интернет-архитектуре . Аутентификация объекта.
29. Аутентификация источника данных. Использование аутентификации уровнями ЭМВОС и Интернет-архитектуры.
30. Защита процедуры аутентификации. Атаки типа «прослушивание/повторная передача». Атаки типа «повторная передача одной и той же проверяющей стороне»
31. Аутентификация. Атаки типа «повторная передача разным проверяющим сторонам». Атаки типа «перехват/повторная передача».
32. Теоретические основы управления доступом. Общие положения. Цель управления доступом
33. Основные аспекты управления доступом. Распределение компонентов управления доступом. Распределение компонентов управления доступом в нескольких ССБ.
34. Угрозы управления доступом. Политики управления доступом
35. Отображение политики УД. Управление политиками. Детализация и локализация. Унаследованные правила
36. Приоритет среди правил ПЛУД. Правила ПЛУД в режиме «по умолчанию». Отображение политики среди взаимодействующих ССБ.
37. Классификация способов управления доступом
38. Схема управления доступом на основе списков доступа
39. Мандатная схема управления доступом
40. Схема управления доступом на основе меток безопасности
41. Контекстная схема управления доступом
42. Взаимодействие управления доступом с другими СЛБ и СПБ: аутентификации, обеспечения целостности данных, обеспечения конфиденциальности данных, аудит.
43. Управление доступом в ЭМВОС и Интернет-архитектуре.
44. Использование управления доступом в рамках уровней ЭМВОС и Интернет-архитектуры.
45. Распределение компонентов управления доступом . Реализационные аспекты. Размещение ФПРИ- и ФПРР-модулей
46. Теоретические основы обеспечения неотказуемости. Общие положения. Основные концепции обеспечения неотказуемости
47. Фазы процедуры обеспечения неотказуемости
48. Политики обеспечения неотказуемости
49. Средства обеспечения неотказуемости .
50. Способы обеспечения неотказуемости. .
51. Службы обеспечения неотказуемости, использующая маркеры безопасности (защитные конверты) ДТС .

52. Служба обеспечения неотказуемости, использующие маркеры безопасности и модули, защищающие от несанкционированного вмешательства.
53. Служба обеспечения неотказуемости, использующая ЭЦП
54. Служба обеспечения неотказуемости, использующие метки времени. СЛНТ, промежуточную доверенную третью сторону. СЛНТ, использующая нотариальное заверение.
55. Угрозы служб обеспечения неотказуемости.
56. Службы обеспечения неотказуемости в системах ЭМВОС и Интернет-архитектуры. Служба обеспечения неотказуемости с подтверждением источника данных. Служба обеспечения неотказуемости с подтверждением доставки данных
57. СЛНТ в системах хранения и ретрансляции
58. Восстановление в службе обеспечения неотказуемости. Взаимодействие со службой единого каталога.
59. Теоретические основы обеспечения конфиденциальности. Общие положения. Основные концепции обеспечения конфиденциальности.
60. Классы служб обеспечения конфиденциальности.
61. Типы способов обеспечения конфиденциальности
62. Угрозы конфиденциальности
63. Типы атак на конфиденциальность.
64. Политики обеспечения конфиденциальности
65. Отображение (описание) политики конфиденциальности
66. Вспомогательная информация и средства обеспечения конфиденциальности.
67. Способы обеспечения конфиденциальности. Обеспечение конфиденциальности на основе предотвращения доступа.
68. Обеспечение конфиденциальности на основе шифрования.
69. Обеспечение конфиденциальности на основе контекстно-зависимого размещения.
70. Обеспечение конфиденциальности в ЭМВОС и Интернет-архитектуре.
71. Теоретические основы обеспечения целостности. Общие положения. Основные концепции обеспечения целостности
72. Типы служб обеспечения целостности
73. Типы способов обеспечения целостности
74. Угрозы целостности.
75. Типы атак на целостность
76. Политики обеспечения целостности. Описание политики.
77. Вспомогательная информация и средства обеспечения целостности. ВИ, необходимая для обеспечения целостности. Средства обеспечения целостности.
78. Классификация способов обеспечения целостности. Обеспечение целостности на основе криптографии.
79. Обеспечение целостности на основе контекста сообщения.
80. Обеспечение целостности на основе обнаружения нарушений и передачи ответных квитанций.
81. Обеспечение целостности путем препятствования (предотвращения)
82. Обеспечение целостности в ЭМВОС и Интернет-архитектуре. Целостность соединения с восстановлением. Целостность соединения без восстановления. Целостность отдельных полей при виртуальном соединении
83. Целостность внешних данных
84. Теоретические основы аудита безопасности и оповещения об опасности. Общие положения. Модель и функции
85. Фазы процедур аудита безопасности и оповещения об опасности

86. Корреляция аудиторской информации и другие аспекты аудита безопасности и оповещения об опасности.
87. Общие принципы АДБ и СОП в ЭМВОС и Интернет-архитектуре
88. Реализация модели АДБ и СОП
89. Регистрация времени возникновения событий, подлежащих аудиторскому контролю
90. Теоретические основы обеспечения ключами. Общая модель обеспечения ключами. Общие положения. Защита ключей
91. Общая модель жизненного цикла ключа
92. Основные концепции обеспечения ключами.
93. Службы (услуги по) обеспечения(ю) ключами обеспечивающие службы (услуги).
94. Концептуальные модели распределения ключей между двумя взаимодействующими сторонами. Общие положения. Распределение ключей между связанными объектами
95. Распределение ключей в рамках одного ССБ.
96. Распределение ключей между двумя ССБ .
97. Провайдеры специализированных услуг
98. Угрозы системе обеспечения ключами
99. Информационные объекты в службе обеспечения ключами
100. Классы прикладных криптографических систем
101. Единая классификация криптографических систем
102. Службы аутентификации, обеспечения целостности и ключи
103. Служба обеспечения конфеденциальности и ключи
104. Обеспечение жизненного цикла СЕРТ|ОК. Общие положения. Удостоверяющий центр
105. Процедура сертификации открытого ключа.
106. Распределение и использование СЕРТ|О К
107. Аннулирование сертификатов открытого ключа

Зачеты и экзамены могут быть проведены в письменной форме, а также в письменной форме с устным дополнением ответа. Зачеты служат формой проверки качества выполнения студентами лабораторных работ, усвоения семестрового учебного материала по дисциплине (модулю), практических и семинарских занятий (при отсутствии экзамена по дисциплине).

По итогам зачета, соответствии с модульно – рейтинговой системой университета, выставляются баллы с последующим переходом по шкале баллы – оценки за зачет, выставляемый как по наименованию «зачтено», «не зачтено», так и дифференцированно т.е. с выставлением отметки по схеме – «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», определяемое решением Ученого совета университета и прописываемого в учебном плане.

Экзамен по дисциплине (модулю) служит для оценки работы студента в течении семестра (года, всего срока обучения и др.) и призван выявить уровень, качество и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умения синтезировать полученные знания и применять их в решении практических задач. По итогам экзамена, в соответствии с модульно – рейтинговой системой университета выставляются баллы, с последующим переходом по шкале оценок на оценки: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», свидетельствующие о приобретенных компетенциях или их отсутствии.

Форма экзаменационного билета (пример оформления)

Министерство науки и высшего образования РФ

ФГБОУ ВО "Дагестанский государственный технический университет"

Дисциплина (модуль) **Информационная безопасность открытых систем**
Код, специальность 10.05.03 Информационная безопасность автоматизированных систем .....
Специализация Безопасность открытых информационных систем
Кафедра ИБ Курс 5 Семестр А
Форма обучения – очная

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1.

1. Службы обеспечения неотказуемости в системах ЭМВОС и Интернет-архитектуры. Служба обеспечения неотказуемости с подтверждением источника данных. Служба обеспечения неотказуемости с подтверждением доставки данных
2. Распределение ключей между двумя ССБ .
3. Провайдеры специализированных услуг

Экзаменатор.....ФИО.

Утвержден на заседании кафедры (протокол №___ от _____20___ г.)

Зав. кафедрой (название) .....ФИО.

В ФОС размещается пример заполненного экзаменационного билета. Весь комплект экзаменационных билетов по дисциплине хранится на кафедре в соответствии с утвержденной номенклатурой дел.

Критерии оценки уровня сформированности компетенций по результатам проведения зачета:

- оценка «зачтено»: обучающийся демонстрирует всестороннее, систематическое и глубокое знание материала, свободно выполняет задания, предусмотренные программой дисциплины, усвоивший основную и дополнительную литературу. Обучающийся выполняет задания, предусмотренные программой дисциплины, на уровне не ниже базового;

- оценка «не зачтено»: обучающийся демонстрирует незнание материала, не выполняет задания, предусмотренные программой дисциплины. Обучающийся не выполняет задания, предусмотренные программой дисциплины, на уровне ниже базового. Дальнейшее освоение ОПОП не возможно без дополнительного изучения материала и подготовки к зачету.

Критерии оценки уровня сформированности компетенций по результатам проведения дифференцированного зачёта (зачета с оценкой) / экзамена:

- оценка **«отлично»:** обучающийся дал полный, развернутый ответ на поставленный вопрос, проявил совокупность осознанных знаний об объекте, доказательно раскрыл

основные положения темы. В ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, явлений. Обучающийся подкрепляет теоретический ответ практическими примерами. Ответ сформулирован научным языком, обоснована авторская позиция обучающегося. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа или с помощью «наводящих» вопросов преподавателя. Обучающимся продемонстрирован высокий уровень владения компетенцией(-ями);

- оценка **«хорошо»:** обучающимся дан полный, развернутый ответ на поставленный вопрос, проявлено умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, но есть недочеты в формулировании понятий, решении задач. При ответах на дополнительные вопросы допущены незначительные ошибки. Обучающимся продемонстрирован повышенный уровень владения компетенцией(-ями);

- оценка **«удовлетворительно»:** обучающимся дан неполный ответ на вопрос, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, явлений, нарушена логика ответа, не сделаны выводы. Речевое оформление требует коррекции. Обучающийся испытывает затруднение при ответе на дополнительные вопросы. Обучающимся продемонстрирован базовый уровень владения компетенцией(-ями);

- оценки **«неудовлетворительно»:** обучающийся испытывает значительные трудности в ответе на вопрос, допускает существенные ошибки, не владеет терминологией, не знает основных понятий, не может ответить на «наводящие» вопросы преподавателя. Обучающимся продемонстрирован низкий уровень владения компетенцией(-ями).