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 «Безопасность операционных 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 _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБ «20» сентября 2021г., протокол №_2

Зав. кафедрой _____ Качаева Г.И.
подпись (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 «Безопасность операционных 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 «Безопасность операционных систем» предусмотрено формирование следующих компетенций:

ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

Код компетенции	**Наименование компетенции**	**Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)**
ОПК-10.	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1.1 знает принципы организации и структуру систем защиты информации современных операционных систем
		ОПК-10.1.2 знает критерии оценки эффективности и надежности систем защиты информации операционных систем
		ОПК-10.2.1 умеет конфигурировать параметры системы защиты информации современных операционных систем
		ОПК-10.2.2 умеет контролировать эффективность принятых мер по реализации политик безопасности информации в современных операционных системах
ОПК-12.	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.1.1 знает принципы построения и функционирования, примеры реализаций современных операционных систем
		ОПК-12.2.1 умеет оценивать эффективность и надежность защиты операционных систем
ОПК-15.	Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1.1 знает принципы организации и структуру систем защиты информации современных операционных систем
		ОПК-15.2.1 умеет проводить установку и настройку современных операционных систем с учетом требований по обеспечению информационной безопасности
		ОПК-15.2.2 умеет использовать средства операционных

		систем для обеспечения безопасного функционирования автоматизированных систем
		ОПК-15.2.3 умеет восстанавливать операционные системы после сбоев

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-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1.1 знает принципы организации и структуру систем защиты информации современных операционных систем	Знать: принципы построения и функционирования, примеры реализаций современных операционных систем;. Уметь: использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; Владеть: профессиональной терминологией в области информационной безопасности;– навыками работы с операционными системами семейств UNIX и Windows, восстановление операционных систем после сбоев;	№№1-34
	ОПК-10.1.2 знает критерии оценки эффективности и надежности систем защиты информации операционных систем		
	ОПК-10.2.1 умеет конфигурировать параметры системы защиты информации современных операционных систем		
	ОПК-10.2.2 умеет контролировать эффективность принятых мер по реализации политик безопасности информации в современных операционных системах		
ОПК-12. Способен применять знания в области безопасности вычислительных сетей,	ОПК-12.1.1 знает принципы построения и функционирования, примеры	Знать: функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;	№№1-34

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

операционных систем и баз данных при разработке автоматизированных систем	реализаций современных операционных систем ОПК-12.2.1 умеет оценивать эффективность и надежность защиты операционных систем	Уметь: оценивать эффективность и надежность защиты операционных систем; Владеть: навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности;	
ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1.1 знает принципы организации и структуру систем защиты информации современных операционных систем ОПК-15.2.1 умеет проводить установку и настройку современных операционных систем с учетом требований по обеспечению информационной безопасности ОПК-15.2.2 умеет использовать средства операционных систем для обеспечения безопасного функционирования автоматизированных систем ОПК-15.2.3 умеет восстанавливать операционные системы после сбоев	Знать: критерии оценки эффективности и надежности средств защиты операционных систем; – принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows; Уметь: планировать политику безопасности операционных систем; Владеть: навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.	№№1-34

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Безопасность операционных 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-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1.1 знает принципы организации и структуру систем защиты информации современных операционных систем	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-10.1.2 знает критерии оценки эффективности и надежности систем защиты информации операционных систем						
	ОПК-10.2.1 умеет конфигурировать параметры системы защиты информации современных операционных систем						
	ОПК-10.2.2 умеет контролировать эффективность принятых мер по реализации политик безопасности информации в современных операционных системах						
ОПК-12. Способен применять знания в	ОПК-12.1.1 знает принципы построения и	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	функционирования, примеры реализаций современных операционных систем ОПК-12.2.1 умеет оценивать эффективность и надежность защиты операционных систем						
ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1.1 знает принципы организации и структуру систем защиты информации современных операционных систем ОПК-15.2.1 умеет проводить установку и настройку современных операционных систем с учетом требований по обеспечению информационной безопасности ОПК-15.2.2 умеет использовать средства операционных систем для обеспечения безопасного функционирования автоматизированных систем ОПК-15.2.3 умеет восстанавливать операционные системы после сбоев	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

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 Безопасность операционных 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 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	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
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

Семестр 4

3.1. Вопросы для входной контрольной работы

1. Дать определение и характеристику основных режимов работы, дисциплин и режимов обслуживания заявок в вычислительных системах.
2. Дать определение и характеристику классов программных средств.
3. Изложить классификацию ОС.
4. Охарактеризовать основные принципы построения ОС.
5. Перечислить виды интерфейсов ОС. Охарактеризовать пакетную технологию как интерфейс. Дать описание интерфейса командной строки.
6. Дать описание графических интерфейсов. В каких ОС они применяются?
7. Охарактеризовать речевую технологию как интерфейс.
8. Охарактеризовать биометрическую технологию как интерфейс.
9. Охарактеризовать семантический интерфейс.

3.2. Контрольные работы по проверке текущих знаний студентов

3.2.1. Аттестационная контрольная работа №1

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Предмет защиты информации.
3. Основные положения безопасности информационных систем.
4. Основные принципы обеспечения информационной безопасности в информационных системах
5. Угрозы безопасности информации в информационно-вычислительных системах
6. Анализ угроз информационной безопасности.

3.2.2. Аттестационная контрольная работа №2

1. Методы обеспечения информационной безопасности.
2. Классификация злоумышленников
3. Основные направления и методы реализации угроз информационной безопасности.
4. Угрозы безопасности ОС.
5. Классификация угроз безопасности ОС. Наиболее распространенные угрозы
6. Программно-технический уровень информационной безопасности
7. Основные понятия программно-технического уровня информационной безопасности.
8. Требования к защите компьютерной информации. Классификация требований к системам защиты.
9. Формализованные требования к защите информации от НСД.

3.2.3. Аттестационная контрольная работа №3

1. Общие подходы к построению систем защиты компьютерной информации.
2. Различия требований и основополагающих механизмов защиты от НСД
3. Требования к защите ОС.
4. Понятие защищенной ОС.
5. Подходы к организации защиты ОС и их недостатки.
6. Этапы построения защиты. Административные меры защиты.
7. Стандарты безопасности ОС

8. Анализ выполнения современными ОС формализованных требований к защите информации от НСД.
9. Анализ существующей статистики угроз для современных универсальных ОС
10. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.

3.3. Оценочные средства для проведения итоговой формы контроля

Вопросы к зачету по дисциплине «Безопасность операционных систем»

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Основные положения безопасности информационных систем.
3. Угрозы безопасности информации в информационно-вычислительных системах
4. Анализ угроз информационной безопасности.
10. Методы обеспечения информационной безопасности.
11. Угрозы безопасности ОС.
12. Классификация угроз безопасности ОС. Наиболее распространенные угрозы
13. Программно-технический уровень информационной безопасности
14. Основные понятия программно-технического уровня информационной безопасности.
11. Различия требований и основополагающих механизмов защиты от НСД
12. Требования к защите ОС.
13. Понятие защищенной ОС.
14. Подходы к организации защиты ОС и их недостатки.
15. Этапы построения защиты. Административные меры защиты.
16. Стандарты безопасности ОС
17. Анализ существующей статистики угроз для современных универсальных ОС

Семестр 5

3.4. Вопросы для входной контрольной работы

1. Основные положения безопасности информационных систем.
2. Анализ угроз информационной безопасности.
3. Угрозы безопасности ОС.
4. Классификация угроз безопасности ОС. Наиболее распространенные угрозы
5. Основные понятия программно-технического уровня информационной безопасности.
6. Различия требований и основополагающих механизмов защиты от НСД
7. Требования к защите ОС.
8. Понятие защищенной ОС.
9. Подходы к организации защиты ОС и их недостатки.
10. Этапы построения защиты. Административные меры защиты.
11. Стандарты безопасности ОС

3.2.4. Аттестационная контрольная работа №4

1. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС
2. Понятия идентификации и аутентификации пользователей.
3. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей.
4. Аутентификация на основе внешних носителей ключа, биометрических

характеристик пользователя.
5. Примеры реализации идентификации и аутентификации в современных ОС.
6. POSIX-совместимые операционные системы. Особенности архитектуры. История развития. Общая характеристика языка командного интерпретатора POSIX-совместимых ОС.
7. Переменные языка командного интерпретатора POSIX-совместимых ОС и их использование. Встроенные переменные

3.2.5. Аттестационная контрольная работа №5

1. Управление порядком выполнения действий в языке командного интерпретатора POSIX-совместимых ОС. Команды для работы с файлами, каталогами, процессами, перенаправление ввода-вывода.
2. Отладка сценариев. Назначение и функции систем выполнения сценариев Windows. Объектные модели и языки систем выполнения сценариев ОС Windows.
3. Удаленное выполнение сценариев ОС Windows. Цифровая подпись сценариев в ОС Windows.
4. Классификация угроз безопасности ОС. Наиболее распространенные угрозы.
5. Понятие защищенной ОС.
6. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.
7. Стандарты безопасности ОС. Виртуальные машины. Изоляция процессов и пользователей.

3.2.6. Аттестационная контрольная работа №6

1. Политики безопасности в ОС Windows
2. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.
3. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС.
4. Понятия идентификации, аутентификации и учета. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей
5. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации, аутентификации и учета в современных ОС.
6. Необходимость аудита. Требования к подсистеме аудита.
7. Централизованный аудит. Штатный аудит в ОС Windows.
8. Реализации аудита в современных ОС.

3.5. Оценочные средства для проведения итоговой формы контроля

Вопросы к зачету по дисциплине «Безопасность операционных систем»

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Предмет защиты информации.
3. Основные положения безопасности информационных систем.
4. Основные принципы обеспечения информационной безопасности в информационных системах
5. Угрозы безопасности информации в информационно-вычислительных системах
6. Анализ угроз информационной безопасности.
7. Методы обеспечения информационной безопасности.

8. Классификация злоумышленников
9. Основные направления и методы реализации угроз информационной безопасности.
10. Угрозы безопасности ОС.
11. 11 .Классификация угроз безопасности ОС. Наиболее распространенные угрозы
12. Программно-технический уровень информационной безопасности
13. Основные понятия программно-технического уровня информационной безопасности.
14. Требования к защите компьютерной информации. Классификация требований к системам защиты.
15. Формализованные требования к защите информации от НСД.
16. Общие подходы к построению систем защиты компьютерной
17. информации.
18. Различия требований и основополагающих механизмов защиты от НСД
19. Требования к защите ОС.
20. Понятие защищенной ОС.
21. Подходы к организации защиты ОС и их недостатки.
22. Этапы построения защиты. Административные меры защиты.
23. Стандарты безопасности ОС
24. Анализ выполнения современными ОС формализованных требований к защите информации от НСД.
25. Анализ существующей статистики угроз для современных универсальных ОС
26. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС
27. Понятия идентификации и аутентификации пользователей.
28. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей.
29. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя.
30. Примеры реализации идентификации и аутентификации в современных ОС.
31. Р081Х-совместимые операционные системы. Особенности архитектуры. История развития. Общая характеристика языка командного интерпретатора POSIX-совместимых ОС.
32. Переменные языка командного интерпретатора POSIX-совместимых ОС и их использование. Встроенные переменные
33. Управление порядком выполнения действий в языке командного интерпретатора POSIX-совместимых ОС. Команды для работы с файлами, каталогами, процессами, перенаправление ввода-вывода.
34. 34.Отладка сценариев. Назначение и функции систем выполнения сценариев Windows. Объектные модели и языки систем выполнения сценариев ОС Windows.
35. Удаленное выполнение сценариев ОС Windows. Цифровая подпись сценариев в ОС Windows.
36. Классификация угроз безопасности ОС. Наиболее распространенные угрозы.
37. Понятие защищенной ОС.
38. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.
39. Стандарты безопасности ОС. Виртуальные машины. Изоляция процессов и пользователей.
40. Политики безопасности в ОС Windows
41. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации, аутентификации и учета в современных ОС.
42. Централизованный аудит. Штатный аудит в ОС Windows.
43. Реализации аудита в современных ОС.

3.6. Вопросы для контроля остаточных знаний по дисциплине «Безопасность операционных систем»

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Основные положения безопасности информационных систем.
3. Основные принципы обеспечения информационной безопасности в информационных системах
4. Основные направления и методы реализации угроз информационной безопасности.
5. Основные понятия программно-технического уровня информационной безопасности.
6. Методы обеспечения информационной безопасности.
7. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.
8. Понятие защищенной ОС.
9. Стандарты безопасности ОС.
10. Подходы к организации защиты ОС и их недостатки.
11. Общие подходы к построению систем защиты компьютерной информации.
12. Понятия идентификации и аутентификации пользователей.
13. Политики безопасности в ОС Windows
14. Реализации аудита в современных ОС.

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) **Управление информационной безопасностью**
Код, специальность 10.05.03 Информационная безопасность автоматизированных систем .....
Специализация Безопасность открытых информационных систем
Кафедра ИБ Курс 4 Семестр 7
Форма обучения – очная

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1.

1. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса.
2. Модель угроз и модель нарушителя.

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).