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 «Организация работы администратора безопасности автоматизированных систем»

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

для направления **10.03.01 Информационная безопасность**
(код, наименование направления подготовки/специальности)

по специализации **Безопасность автоматизированных систем**
(наименование)

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

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

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

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств 3

2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля) 3

2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП ... 4

2.1.2. Этапы формирования компетенций 6

2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания 8

2.2.1. Показатели уровней сформированности компетенций на этапах их формирования 8

2.2.2. Описание шкал оценивания 10

3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП 11

3.1. Задания и вопросы для входного контроля 11

3.2. Оценочные средства и критерии сформированности компетенций 11

3.2.1.Аттестационная контрольная работа №1 11

3.2.2.Перечень вопросов на зачет 11

3.2.3.Вопросы проверки остаточных знаний 12

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины Организация работы администратора безопасности автоматизированных 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 направлению 10.03.01 Информационная безопасность.

Рабочей программой дисциплины Организация работы администратора безопасности автоматизированных систем предусмотрено формирование следующей компетенции:

УК-1-Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

ПК-1-Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации.

ПК-2-Способен осуществлять администрироование средств защиты информации в компьютерных системах и сетях.

ПК-3-Способен осуществлять администрирование подсистем защиты информации в операционных системах.

ПК-4-Способен осуществлять аудит защищенности информации в автоматизированных системах.

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)

- *Контрольная работа*
- *Решение задач (заданий)*
- *Тест (для текущего контроля)*
- *Устный опрос*
- *Задания / вопросы для проведения зачета*

Перечень оценочных средств при необходимости может быть дополнен.

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 тем[1]
УК-1-Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.3 - знает основные источники информации о проблемных ситуациях в профессиональной деятельности и подходы к критическому анализу этой информации	знает основные источники информации о проблемных ситуациях в профессиональной деятельности и подходы к критическому анализу этой информации	№№1-8
	УК-1.5 - умеет критически анализировать проблемные ситуации и вырабатывать стратегию действий в ходе решения профессиональных задач	умеет критически анализировать проблемные ситуации и вырабатывать стратегию действий в ходе решения профессиональных задач	№№1-8
ПК-1-Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации	ПК – 1.1 знать принципы построения компьютерных систем и сетей	знать принципы построения компьютерных систем и сетей	№№1-8
	ПК – 1.2 знать принципы построения систем обнаружения компьютерных атак	знать принципы построения систем обнаружения компьютерных атак	№№1-8
	ПК – 1.3 уметь применять инструментальные средства проведения мониторинга защищенности компьютерных систем	уметь применять инструментальные средства проведения мониторинга защищенности компьютерных систем	№№1-8
	ПК – 1.4 владеть правилами составления отчетов по результатам проверок	владеть правилами составления отчетов по результатам проверок	№№1-8
ПК-2-Способен осуществлять администрироование средств защиты информации в компьютерных системах и сетях	ПК – 2.1 знать методы выявления каналов утечки информации	знать методы выявления каналов утечки информации	№№1-8
	ПК – 2.2 уметь формировать модели угроз и модели нарушителя безопасности компьютерных систем	уметь формировать модели угроз и модели нарушителя безопасности компьютерных систем	№№1-8
	ПК -2.3 Уметь осуществлять принятие решений о необходимости использования программно-аппаратных	уметь осуществлять принятие решений о необходимости использования программно-аппаратных средств защиты информации	№№1-8

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

	средств защиты информации		
	ПК –2.4 владеть организационными мерами по защите информации	владеть организационными мерами по защите информации	№№1-8
ПК-3-Способен осуществлять администрирование подсистем защиты информации в операционных системах	ПК –3.1 знать принципы построения и функционирования систем и сетей передачи информации	знать принципы построения и функционирования систем и сетей передачи информации	№№1-8
	ПК -3.2 знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	№№1-8
	ПК – 3.3 уметь анализировать основные узлы и устройства современных автоматизированных систем	уметь анализировать основные узлы и устройства современных автоматизированных систем	№№1-8
	ПК – 3.4 владеть организационными мерами по защите информации	3.4 владеть организационными мерами по защите информации	№№1-8
ПК-4-Способен осуществлять аудит защищенности информации в автоматизированных системах	ПК – 4.1 знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	№№1-8
	ПК – 4.2 уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации	уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации	№№1-8
	ПК – 4.3 – уметь осуществлять разработку отчетных документов и разделов технических заданий	уметь осуществлять разработку отчетных документов и разделов технических заданий	№№1-8
	ПК – 4.4 анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами	анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами	№№1-8

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Организация работы администратора безопасности автоматизированных 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
УК-1-Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.3 - знает основные источники информации о проблемных ситуациях в профессиональной деятельности и подходы к критическому анализу этой информации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	УК-1.5 - умеет критически анализировать проблемные ситуации и вырабатывать стратегию действий в ходе решения профессиональных задач	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
ПК-1-Способен обеспечивать защиту информации в автоматизированных системах	ПК – 1.1 знать принципы построения компьютерных систем и сетей	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК – 1.2 знать принципы построения систем обнаружения компьютерных атак	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК – 1.3 уметь применять инструментальные средства проведения мониторинга	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос

в процессе их эксплуатации	защищенности компьютерных систем						
	ПК – 1.4 владеть правилами составления отчетов по результатам проверок	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
ПК-2-Способен осуществлять администрирование средств защиты информации в компьютерных системах и сетях	ПК – 2.1 знать методы выявления каналов утечки информации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК – 2.2 уметь формировать модели угроз и модели нарушителя безопасности компьютерных систем	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК -2.3 Уметь осуществлять принятие решений о необходимости использования программно-аппаратных средств защиты информации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК –2.4 владеть организационными мерами по защите информации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
ПК-3-Способен осуществлять администрирование подсистем защиты информации в операционных системах	ПК –3.1 знать Принципы построения и функционирования систем и сетей передачи информации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК -3.2 знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК – 3.3 уметь анализировать основные узлы и устройства современных автоматизированных систем	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК – 3.4 владеть организационными мерами по защите информации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
ПК-4-Способен осуществлять аудит защищенности информации в автоматизированных системах	ПК – 4.1 знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК – 4.2 уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК – 4.3 – уметь осуществлять разработку отчетных документов и разделов технических заданий	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК – 4.4 анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос

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 Организация работы администратора безопасности автоматизированных 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
Базовый (оценка «удовлетворительно», «зачтено»)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП.	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные,

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	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. 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. Локальные сети
10. Глобальные сети
11. Цифровые сети с интеграцией услуг (ISDN – ЦСИС)
12. Особенности защищенных телекоммуникационных сетей
13. Маршрутизация и управление в телекоммуникационных сетях
14. Стратегии межсетевого взаимодействия.
15. Теоретические основы автоматизации управления.
16. Методы проектирования автоматизированных систем.

3.2. Оценочные средства и критерии сформированности компетенций

3.2.1.Аттестационная контрольная работа №1

1. IP-адресация.
2. Разбиение IP-сетей на подсети и создание надсетей.
3. Установка и конфигурирование TCP/IP на примере Windows Server 2008.
4. Анализ сетевого трафика средствами «Сетевого монитора».
5. Устранение неполадок подключений TCP/IP.
6. Сравнение DNS и NetBIOS.
7. DNS в сетях Windows Server 2008.
8. Развертывание DNScерверов.
9. Настройка DNS-клиентов.
10. Настройка параметров DNS-сервера.
11. Настройка свойств зоны и передачи.
12. Настройка дополнительных свойств DNS-сервера.
13. Основные понятия теории защиты информации; угрозы безопасности; математические модели политики безопасности; общие критерии безопасности информационных технологий
14. Средства устранения неполадок DNS.
15. Средства мониторинга DNS.

3.2.2.Перечень вопросов на зачет

1. Разбиение IP-сетей на подсети и создание надсетей.
2. Установка и конфигурирование TCP/IP на примере Windows Server 2008.
3. Анализ сетевого трафика средствами «Сетевого монитора».
4. Устранение неполадок подключений TCP/IP.
5. Сравнение DNS и NetBIOS.
6. DNS в сетях Windows Server 2008.
7. Развертывание DNScерверов.
8. Настройка DNS-клиентов.
9. Настройка параметров DNS-сервера.

10. Настройка свойств зоны и передачи.
11. Настройка дополнительных свойств DNS-сервера.
12. Основные понятия теории защиты информации; угрозы безопасности; математические модели политики безопасности; общие критерии безопасности информационных технологий
13. Средства устранения неполадок DNS.
14. Средства мониторинга DNS.
15. Специальные проверки.
16. Порядок проведения специальной проверки технических средств
17. Аутентификация данных; алгоритмы безопасного хеширования;
18. ЭЦП криптосистем RSA и Эль Гамаля; алгоритм цифровой подписи DSA; отечественные алгоритмы цифрой подписи
19. Анализ DHCP-трафика.
20. Мониторинг DHCP с применением журнала аудита.
21. Устранение неполадок DHCP.
22. Настройка Windows Server 2008 для маршрутизации в локальной сети.
23. Настройка маршрутизации вызовов по требованию.

3.2.3.Вопросы проверки остаточных знаний

1. Введение в администрирование в ИС.
2. Функции и процедуры администрирования.
3. Службы администрирования.
4. Эксплуатация и сопровождение информационных систем.
5. Инсталляция информационных систем.
6. Оперативное управление и регламентные работы.
7. Управление и обслуживание технических средств.
8. Аппаратно-программные платформы администрирования операционных систем.
9. Аппаратно-программные платформы администрирования баз данных.
10. Аппаратно-программные платформы администрирования службы каталогов.
11. Уровни и модели TCP/IP
12. Организация сетевого трафика
13. Сравнение DNS и NetBIOS
14. Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности
15. Ошибки DNS
16. Мероприятия по выявлению каналов утечки информации
17. Методы идентификации и аутентификации пользователей компьютерных систем.

Критерии оценки уровня сформированности компетенций при проведении деловой (ролевой) игры:

- оценка «отлично» выставляется обучающемуся (члену группы), если в процессе решения проблемной ситуации (игры) продемонстрированы глубокие знания дисциплины, сущности проблемы, даны логически последовательные, содержательные, полные, правильные и конкретные ответы на все вопросы; даны рекомендации по использованию данных в будущем для аналогичных ситуаций;

- оценка «хорошо» выставляется обучающемуся (члену группы), если все рассуждения и обоснования верны, однако, имеются незначительные неточности, представлен недостаточно полный выбор стратегий поведения/методов/инструментов (в части обоснования);

- оценка «удовлетворительно» выставляется обучающемуся (члену группы), слабо ориентирующемуся в материале; в рассуждениях обучающийся не демонстрирует логику ответа, плохо владеет профессиональной терминологией, не раскрывает суть проблемы и не предлагает конкретного ее решения; обучающийся не принимает активного участия в работе группы, выполнившей задание на «хорошо» или «отлично»;

- оценка «неудовлетворительно» выставляется обучающемуся (члену группы), не принимавшему участие в работе группы или группе, не справившейся с заданием на уровне, достаточном для проставления положительной оценки.

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.

Критерии оценки уровня сформированности компетенций для проведения экзамена/дифференцированного зачёта (зачета с оценкой) зависят от их форм проведения (тест, вопросы, задания, решение задач и т.д.).