

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Баламирзоев Назим Лиодинович
Должность: Ректор
Дата подписания: 06.04.2026 13:46:56
Уникальный программный ключ:
5cf0c6f89e80f49a334f6a4ba58e91f3326b9926

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 «Организационное и правовое обеспечение информационной безопасности»

Уровень образования	<u>специалитет</u> <small>(бакалавриат/магистратура/специалитет)</small>
Специальность	<u>10.05.03 Информационная безопасность автоматизированных систем</u> <small>(код, наименование специальности)</small>
Специализация	<u>Безопасность открытых информационных систем</u> <small>(наименование)</small>

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.....	18
2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)	18
2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП.....	19
2.1.1. Этапы формирования компетенций.....	20
2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания.....	21
2.2.1. Показатели уровней сформированности компетенций на этапах их формирования	21
2.2.2. Описание шкал оценивания.....	23
3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП.....	24
3.1. Задания и вопросы для входного контроля.....	24
3.2. Задания для промежуточной аттестации (зачета и (или) экзамена)	24
3.2.1. Аттестационная контрольная работа №1	24
3.2.2. Аттестационная контрольная работа №2	24
3.2.3. Аттестационная контрольная работа №3	24
3.3. Список вопросов к зачету и (или) / экзамену.....	24
3.4. Вопросы для проверки остаточных знаний по дисциплине «Организационное и правовое обеспечение информационной безопасности»	25

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Организационное и правовое обеспечение информационной безопасности» 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 «Организационное и правовое обеспечение информационной безопасности» предусмотрено формирование следующих компетенций:

ПК-4 - Способностью осуществлять формирование требований к защите 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)

- Устный опрос
- Вопросы для проведения зачета

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
ПК-4 - Способен осуществлять формирование требований к защите информации в автоматизированных системах	ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	<p>ПК-4.1.1 Знает руководящие и документы нормативные, методические уполномоченных федеральных органов исполнительной власти по защите информации</p> <p>ПК-4.1.2 Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)</p> <p>ПК-4.1.3 Владеет навыками планирования мероприятий по обеспечению защиты информации и организацию работы персонала автоматизированной системы с учетом требований по защите информации</p>	№№1-17

¹ Наименования разделов и тем должен соответствовать рабочей программе дисциплины.

2.1.1. Этапы формирования компетенций

Сформированность компетенций по дисциплине Организационное и правовое обеспечение информационной безопасности 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)*

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Этапы формирования компетенции					
		Этап текущих аттестаций		Этап промежуточной аттестации		18-20 недели	
		1-5 недели	6-10 недели	11-15 недели	1-17 недели		
1	ОПК-10 Способностью использовать средства криптографической защиты информации при решении задач профессиональной деятельности	2 Текущая аттестация №1	3 Текущая аттестация №2	4 Текущая аттестация №3	5 СРС	6 КР/КП	7 Промежуточная аттестация
ОПК-10 Способностью использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1.5 знает основные задачи и понятия криптографии ОПК-10.1.6 знает модели шифров и математические методы их исследования	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
		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 Организационное и правовое обеспечение информационной безопасности 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 значительными 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 ОППО. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения.	Обучающийся владеет знаниями основного материала на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками.

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Низкий (оценка «неудовлетворительно», «не зачтено»)	Обучающимся продемонстрирован базовый уровень освоения компетенции Демонстрирует полное отсутствие теоретических знаний дисциплины, отсутствие практических умений и навыков	соответствующий минимально необходимому уровню для решения профессиональных задач

Показатели уровня 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 пятибалльная, двадцатибалльная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			Критерии оценивания
пятибалльная	двадцатибалльная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: <ul style="list-style-type: none"> - 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.: <ul style="list-style-type: none"> - 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.: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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. Формальное описание структуры информационной системы.
2. Составление модели угроз информационной системе.
3. Формирование требований к системе защиты информации.
4. Формирование требований к политике информационной безопасности.
5. Формирование регламента действий при возникновении нештатных ситуаций.

3.2. Задания для промежуточной аттестации

3.2.1 Аттестационная контрольная работа №1

1. Организационные основы и принципы деятельности службы защиты информации.
2. Законодательство РФ в области информационной безопасности.
3. Правовые основы защиты конфиденциальной информации.
4. Правовые основы защиты государственной тайны.
5. Лицензирование и сертификация.

3.2.2 Аттестационная контрольная работа №2

1. Нормы ответственности за правонарушения в сфере компьютерных технологий.
2. Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.
3. Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.
4. Структура службы защиты информации.
5. Организационные основы и принципы деятельности службы защиты информации.

3.2.3 Аттестационная контрольная работа №3

1. Сущность, организация и принципы управления службой защиты информации на предприятии.
2. Методы и технологии управления службой защиты информации на предприятии.
3. Средства и методы физической защиты объектов.
4. Организация службы безопасности и работа с кадрами.
5. Организация и обеспечения режима секретности.

3.3. Список вопросов к зачету

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?
10. Организационные основы и принципы деятельности службы защиты информации.
11. Законодательство РФ в области информационной безопасности.
12. Правовые основы защиты конфиденциальной информации.
13. Правовые основы защиты государственной тайны.
14. Лицензирование и сертификация.

15. Нормы ответственности за правонарушения в сфере компьютерных технологий.
16. Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.
17. Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.
18. Структура службы защиты информации.
19. Организационные основы и принципы деятельности службы защиты информации».
20. Сущность, организация и принципы управления службой защиты информации на предприятии.
21. Методы и технологии управления службой защиты информации на предприятии.
22. Средства и методы физической защиты объектов.
23. Организация службы безопасности и работа с кадрами.
24. Организация и обеспечения режима секретности.
25. Организация труда сотрудников подразделения мониторинга информационной безопасности.
26. Организация пропускного и внутри объектового режима.

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.

3.4. Вопросы для проверки остаточных знаний по дисциплине «Организационное и правовое обеспечение информационной безопасности»

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?