

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:
5cf0d6f89e80f49a334f6a4ba58e91f3326b9926

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 защиты персональных данных в информационных системах»

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

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

Фонд оценочных средств обсужден на заседании кафедры ИБиПИ «15» октября 2025г., протокол № 2

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

г. Махачкала 2025

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. Эссе по дисциплине «Организация защиты персональных данных в информационных системах» | 11 |
| 3.2.2. Аттестационная контрольная работа №1 | 11 |
| 3.2.3. Аттестационная контрольная работа №2 | 11 |
| 3.2.4. Аттестационная контрольная работа №3 | 11 |
| 3.2.5. Список вопросов к экзамену | 12 |

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Организация защиты персональных данных в информационных системах» 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 «Организация защиты персональных данных в информационных системах» 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.

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)

- *Эссе*
- *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 |
|---|--|--|---|
| ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства | ОПК-1.1.3 знает источники и классификацию угроз информационной безопасности | Знать: Студент знает источники угроз безопасности персональных данных и их классификацию по нормативным документам ФСТЭК России. Уметь: Студент умеет анализировать информационную систему для выявления актуальных угроз конфиденциальности персональных данных. Владеть: Студент владеет методикой выявления и классификации угроз при разработке модели угроз для конкретной информационной системы. | №№ 1-9 |
| | ОПК-1.1.4 знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации | Знать: Студент знает состав и принципы применения технических и организационных мер защиты персональных данных, регламентированных законодательством РФ. Уметь: Студент умеет подбирать необходимые средства защиты информации для достижения заданного уровня защищенности персональных данных. Владеть: Студент владеет принципами проектирования комплексной системы защиты персональных данных на основе модели угроз. | №№ 1-9 |
| | ОПК-1.1.5 знает основные понятия, связанные с обеспечением информационной безопасности личности, общества и государства, понятия информационного противоборства, | Знать: Студент знает правовые основы и ключевые понятия защиты информационной безопасности личности в контексте обработки персональных данных. Уметь: Студент умеет разграничивать правовые режимы информации и анализировать обязанности оператора персональных данных. Владеть: Студент владеет понятийным аппаратом в области защиты прав субъектов персональных данных и информационной безопасности государства | №№ 1-9 |

¹ Наименования разделов и тем должен соответствовать рабочей программе дисциплины.

| | | | |
|--|---|--|--|
| | информационной войны и формы их проявлений в современном мире | | |
|--|---|--|--|

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Организация защиты персональных данных в информационных системах» 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 промежуточной аттестации |
|---|---|--------------------------------|-----------------------|-----------------------|-------------|--------------|-------------------------------|
| | | Этап текущих аттестаций | | | | 18-20 неделя | |
| | | 1-5 неделя | 6-10 неделя | 11-15 неделя | 1-17 неделя | | |
| | | Текущая аттестация №1 | Текущая аттестация №2 | Текущая аттестация №3 | СРС | | КР/КП |
| 1 | | 2 | 3 | 4 | 5 | 6 | 7 |
| ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства | ОПК-1.1.3 знает источники и классификацию угроз информационной безопасности | Контрольная работа №1 | Контрольная работа №2 | Контрольная работа №3 | | | Вопросы для проведения зачета |
| | ОПК-1.1.4 знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации | Контрольная работа №1 | Контрольная работа №2 | Контрольная работа №3 | | | Вопросы для проведения зачета |
| | ОПК-1.1.5 знает основные понятия, связанные с обеспечением информационной безопасности личности, общества и государства, | Контрольная работа №1 | Контрольная работа №2 | Контрольная работа №3 | | | Вопросы для проведения зачета |

| | | | | | | | |
|--|--|--|--|--|--|--|--|
| | <p>понятия информационного противоборства, информационной войны и формы их проявлений в современном мире</p> | | | | | | |
|--|--|--|--|--|--|--|--|

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 защиты персональных данных в информационных системах» 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 допускает неточности в ответе, но обладает необходимыми знаниями для их | Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения |

| Уровень | Универсальные компетенции | Общепрофессиональные/ профессиональные компетенции |
|---|--|--|
| | устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции | 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 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. Дайте определение понятию «персональные данные» согласно Федеральному закону №152-ФЗ.
2. Назовите базовые принципы обработки персональных данных.
3. Перечислите основные нормативно-правовые акты РФ в области защиты информации.
4. Что такое «угроза безопасности информации»?
5. В чем заключается разница между конфиденциальностью, целостностью и доступностью информации?
6. Назовите основные классы средств защиты информации.
7. Что такое «информационная система персональных данных» (ИСПДн)?

3.2. Оценочные средства и критерии сформированности компетенций

3.2.1. Аттестационная контрольная работа №1

1. Опишите структуру законодательной базы РФ в сфере защиты персональных данных.
2. Раскройте содержание прав и обязанностей субъекта персональных данных.
3. Дайте характеристику категориям персональных данных (общедоступные, биометрические, специальные и т.д.).
4. Каковы условия, при которых обработка ПДн требует письменного согласия субъекта?
5. Перечислите и охарактеризуйте основные угрозы конфиденциальности ПДн.
6. Классифицируйте источники угроз безопасности информации по виду их происхождения.
7. Что подразумевается под «моделью нарушителя» при построении системы защиты?
8. Объясните, чем внутренний нарушитель отличается от внешнего.
9. Назовите цели и этапы проведения оценки угроз безопасности ПДн.
10. Дайте определение понятию «уровень защищенности» ИСПДн.

3.2.3. Аттестационная контрольная работа №2

1. Опишите основные этапы и методологию построения частной модели угроз для конкретной ИСПДн.
2. Какие факторы влияют на выбор актуальных угроз при построении модели?
3. Раскройте назначение и принципы работы электронной цифровой подписи (ЭЦП) в контексте защиты ПДн.
4. В чем заключаются ключевые различия между симметричными и асимметричными криптосистемами?
5. Каковы основные функции и место межсетевых экранов (firewall) в системе защиты информации?
6. Опишите назначение и принцип действия систем обнаружения вторжений (IDS).
7. Какие технические меры применяются для защиты ПДн при их передаче по открытым каналам связи?
8. Перечислите основные классы вредоносного программного обеспечения и механизмы защиты от них.
9. Какие средства защиты информации применяются для обеспечения целостности и доступности данных?
10. Объясните, как использование виртуальных частных сетей (VPN) повышает безопасность передачи данных.

3.2.4. Аттестационная контрольная работа №3

1. Составьте примерный перечень организационно-распорядительных документов, необходимых для защиты ПДн в организации.
2. Раскройте содержание основных мероприятий по работе с персоналом в рамках СЗПДн.
3. Опишите порядок действий оператора при обнаружении инцидента утечки персональных данных.
4. Назовите основные этапы проектирования и внедрения системы защиты персональных данных (СЗПДн).
5. Как определяется необходимый уровень защищенности ИСПДн согласно законодательству РФ?
6. Опишите порядок уведомления Роскомнадзора об обработке ПДн и случаи, когда оно не требуется.
7. Разграничьте полномочия и функции Роскомнадзора, ФСТЭК России и ФСБ России в области контроля за защитой ПДн.
8. Перечислите виды юридической ответственности за нарушение законодательства о персональных данных.
9. Каковы состав и меры административной ответственности за нарушения в сфере ПДн по КоАП РФ?
10. Опишите порядок проведения проверок операторов ПДн уполномоченными органами государственного контроля.

3.2.5. Список вопросов к зачету

1. Дайте развернутую характеристику Федерального закона №152-ФЗ как основы правового регулирования защиты ПДн в РФ.
2. Проанализируйте взаимосвязь Конституции РФ, международных договоров и федеральных законов в системе правового обеспечения защиты ПДн.
3. Объясните принцип законности и целевого ограничения при обработке персональных данных на практическом примере.
4. Сравните правовые режимы различных категорий персональных данных (специальных, биометрических, общедоступных).
5. Классифицируйте угрозы безопасности ПДн для информационной системы интернет-банка. Обоснуйте выбор критериев.
6. Разработайте фрагмент модели нарушителя для внутреннего сотрудника, имеющего легальный доступ к ИСПДн.
7. Спроектируйте последовательность шагов по оценке актуальных угроз для облачной CRM-системы, содержащей данные клиентов.
8. Обоснуйте выбор криптографических алгоритмов (симметричного и асимметричного) для защиты данных в системе электронного документооборота.
9. Сравните эффективность применения ЭЦП и хэш-функций для решения задач аутентификации и обеспечения целостности данных.
10. Опишите архитектуру и принцип построения системы многоуровневой сетевой защиты для распределенной ИСПДн филиалов компании.
11. Предложите комплекс мер защиты от вредоносного ПО и целевых атак (APT) на рабочем месте оператора ПДн.
12. Составьте техническое задание на выбор системы обнаружения и предотвращения вторжений (IPS) для корпоративной сети.
13. Разработайте проект «Положения об обработке и защите персональных данных» для средней коммерческой организации.
14. Составьте программу вводного и периодического инструктажа для сотрудников, работающих с ПДн.

15. Опишите регламент действий службы ИБ при обнаружении попытки несанкционированного доступа к базе данных сотрудников.
16. Спроектируйте основные этапы работ по аудиту и аттестации существующей СЗПДн в организации.
17. На практическом примере определите уровень защищенности ИСПДн и обоснуйте необходимый набор защитных мер.
18. Проанализируйте случаи, когда обработка ПДн может осуществляться без согласия субъекта.
19. Сравните контрольные полномочия Роскомнадзора и ФСТЭК России в отношении одного оператора ПДн.
20. Опишите процедуру рассмотрения жалобы субъекта ПДн на действия оператора уполномоченным органом.
21. Квалифицируйте возможные виды ответственности (дисциплинарную, административную, уголовную) за утечку базы данных клиентов по неосторожности сотрудника.
22. Проанализируйте состав преступления по статье 137 УК РФ «Нарушение неприкосновенности частной жизни».
23. Объясните, какие меры должен предпринять оператор для правомерной трансграничной передачи ПДн.
24. Сформулируйте основные этические дилеммы и профессиональные стандарты специалиста по защите ПДн.
25. Оцените роль международных стандартов (ISO 27001, GDPR) в развитии национального законодательства о ПДн.
26. Разработайте комплексный план мероприятий по приведению деятельности условного интернет-магазина в соответствие с требованиями 152-ФЗ.
27. Проведите сравнительный анализ угроз для традиционной (on-premise) и облачной (SaaS) ИСПДн.
28. Смоделируйте и опишите процесс согласования требований по ИБ между юридическим отделом, службой ИТ и подразделением безопасности.
29. Предложите экономическое обоснование для внедрения СЗПДн, оценив возможные убытки от инцидентов и стоимость защитных мер.
30. Спрогнозируйте тенденции развития угроз и технологий защиты ПДн на ближайшие 5-10 лет.

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.

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).