

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Баламирзоев Назим Лиодинович
Должность: Ректор
Дата подписания: 06.04.2026 13:39:11
Уникальный программный ключ:
5cf0d6f89e80f49a33416a4ba58e91f5326b9926

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 «Методы и средства криптографической защиты информации»

Уровень образования

специалитет

(бакалавриат/магистратура/специалитет)

Специальность

10.05.03 Информационная безопасность
автоматизированных систем

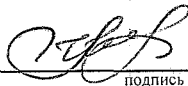
(код, наименование специальности)

Специализация

Безопасность открытых информационных систем

(наименование)

Разработчик



подпись

Качаева Г.И.

(ФИО уч. степень, уч. звание)

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

Зав. кафедрой



подпись

Качаева Г.И.

(ФИО уч. степень, уч. звание)

г. Махачкала 2021

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств.....	19
2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)	19
2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП.....	20
2.1.2. Этапы формирования компетенций.....	21
2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания.....	22
2.2.1. Показатели уровней сформированности компетенций на этапах их формирования	22
2.2.2. Описание шкал оценивания.....	24
3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП.....	25
3.1. Задания и вопросы для входного контроля.....	25
3.2. Оценочные средства и критерии сформированности компетенций	25

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Методы и средства криптографической защиты информации» 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 «Методы и средства криптографической защиты информации» предусмотрено формирование следующих компетенций:

ОПК-10 - Способностью использовать средства криптографической защиты информации при решении задач профессиональной деятельности

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)

- Тест (для текущего контроля)
- Устный опрос
- Тест для проведения зачета / дифференцированного зачета (зачета с оценкой) / экзамена
- Задания / вопросы для проведения зачета / дифференцированного зачета (зачета с оценкой) / 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 тем ¹
ОПК-10 Способностью использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1.5 знает основные задачи и понятия криптографии	Знать: модели шифров и математические методы их исследования; Уметь: применять математические методы описания и исследования криптографических систем; Владеть: навыками математического моделирования в криптографии.	
	ОПК-10.1.6 знает модели шифров и математические методы их исследования	Знать: основные задачи и понятия криптографических методов защиты информации; основные криптографические методы защиты информации; требования к шифрам и основные характеристики шифров; Уметь: осуществлять рациональный выбор криптографических методов и средств защиты информации в телекоммуникационных системах; реализовывать типовые криптографические преобразования; Владеть: навыками использования типовых криптографических преобразований; навыками применения инженерно-криптографических механизмов для обнаружения неисправностей криптографических средств защиты информации	

¹ Наименования разделов и тем должен соответствовать рабочей программе дисциплины.

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Криптографические методы защиты информации 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 Способностью использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1.5 знает основные задачи и понятия криптографии	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	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

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 _____ 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 устранения.	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,

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	Обучающимся продемонстрирован базовый уровень освоения компетенции	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. Системы счисления.
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. Оценочные средства и критерии сформированности компетенций

Курсовая работа/курсовый проект

Примерные темы курсовых работ/курсовых проектов

1. Программная реализация криптографической системы ГОСТ 28147-89;
2. Программная реализация криптографических систем DES, 3-DES и DESX
3. Криптографические функции хеширования;
4. Теоретическая оценка криптозащищенности инфокоммуникационных систем;
5. Моделирование криптозащищенной телекоммуникационной системы;
6. Разработка программы симметричного шифрования-дешифрования информации
7. Российского стандарта шифрования ГОСТ28147-89 ;
8. Разработка программы асимметричного шифрования-дешифрования информации RSA;
9. Разработка модели криптозащищенной телекоммуникационной системы.
10. Модели и методы распознавания открытых текстов.
11. Криптоанализ шифров с помощью генетических алгоритмов.
12. Совершенные имитостойкие шифры.
13. Шифры, близкие к экстремальным.
14. Итеративные блочные шифры.
15. Шифры, не распространяющие искажений.
16. Контроль целостности данных с помощью хеш-функций.
17. Оптимальные коды аутентификации.

Требования к структуре, содержанию и оформлению курсовых работ (проектов) приводятся в методических указаниях/рекомендациях.

Критерии оценки уровня сформированности компетенций при выполнении курсовой работы/курсового проекта:

- оценка «отлично»: продемонстрировано блестящее владение проблемой исследования, материал выстроен логично, последовательно, обучающийся аргументированно отстаивает свою точку зрения. Во введении приводится обоснование выбора конкретной темы, четко определены цель и задачи работы (проекта). Использован достаточный перечень источников и литературы для методологической базы исследования. Обучающийся грамотно использует профессиональные термины, актуальные исходные данные. Проведен самостоятельный анализ (исследование) объекта. По результатам работы сделаны логичные выводы. Оформление работы соответствует методическим рекомендациям. Объем и содержание работы соответствует требованиям. На защите обучающийся исчерпывающе отвечает на все дополнительные вопросы;

- оценка «хорошо»: обучающийся демонстрирует повышенный уровень владения проблемой исследования, логично, последовательно и аргументированно отстаивает ее концептуальное содержание. Во введении содержатся небольшие неточности в формулировках цели, задач. В основной части допущены незначительные погрешности в

расчетах (в исследовании). Выводы обоснованы, аргументированы. Оформление работы соответствует методическим рекомендациям. Объем работы соответствует требованиям. На защите обучающийся отвечает на все дополнительные вопросы;

- оценка «удовлетворительно»: обучающийся демонстрирует базовый уровень владения проблемой исследования. Во введении указаны цель и задачи исследования, но отсутствуют их четкие формулировки. Работа является компиляцией чужих исследований с попыткой формулировки собственных выводов в конце работы. Изложение материала логично и аргументировано. Наблюдается отступление от требований в оформлении и объеме работы. При ответе на вопросы обучающийся испытывает затруднения;

- оценка «неудовлетворительно»: обнаруживается несамостоятельность выполнения курсовой работы, некомпетентность в исследуемой проблеме. Нарушена логика изложения. Работа не соответствует требованиям, предъявляемым к оформлению и содержанию. На защите курсовой работы обучающийся не отвечает на вопросы.

Тест №1 по теме/разделу «Наименование темы/раздела»

- Время выполнения 20 мин.
- Количество вопросов 10 .
- Форма работы – самостоятельная, индивидуальная.

Тест 1 Вариант 1

1. Конфиденциальность защищаемой информации обеспечивается с помощью:
 - a) электронной подписи
 - b) шифрования
 - c) хэш-функции
2. Способность шифра противостоять попыткам противника по имитации или подмене зашифрованной информации называется
 - a) имитостойкостью.
 - b) криптостойкостью.
 - c) помехозащищенностью.
3. Если криптоаналитик может взломать шифр, но не обладает необходимыми вычислительными ресурсами, то считается, что
 - a) шифр является практически стойким.
 - b) шифр является теоретически стойким.
 - c) шифр является практически имитостойким.
4. Если для шифрования и расшифрования используется один и тот же ключ, то шифр является
 - a) симметричным.
 - b) ассиметричным.
 - c) блочным.
5. Шифры, в которых знание ключа шифрования не позволяет определить ключ расшифрования называются
 - a) поточными.
 - b) симметричными.
 - c) ассиметричными.
6. Шифры, в которых каждый символ открытого текста зашифровывается независимо от других называются
 - a) блочными.
 - b) имитозащищенными.
 - c) поточными.
7. Шифрование информации предназначено для обеспечения
 - a) целостности защищаемой информации
 - b) конфиденциальности защищаемой информации

с) доступности защищаемой информации

8. Исходные данные с доступным семантическим содержанием, подлежащие криптографическому преобразованию, называются

- а) открытый текст
- б) шифртекст
- с) имитовставка

9. Параметр шифра, определяющий выбор конкретного варианта преобразования зашифрования или расшифрования из множества преобразований, составляющих шифр, называется...

- а) Алгоритм
- б) шифр
- с) ключ

10. Процесс преобразования шифртекста в открытый текст при неизвестном ключе называется...

- а) дешифрование
- б) зашифрование
- с) расшифрование

Критерии оценки уровня сформированности компетенций при выполнении теста:

Оценка	Показатели*
Отлично	85-100%
Хорошо	70-84%
Удовлетворительно	56-69%
Неудовлетворительно	менее 56%

* - % выполненных заданий от общего количества заданий в тесте. Показатели зависят от уровня сложности тестовых заданий.

Список вопросов к зачету и (или) / экзамену

- 1) Определение шифра. Классификация шифров.
- 2) Понятие криптографической системы. Требования к криптографическим системам.
- 3) Формальные модели шифров. Алгебраическая и вероятностная модель шифра.
- 4) Математическая модель открытых текстов.
- 5) Алгебраическая модель шифра перестановки.
- 6) Алгебраическая модель шифра замены.
- 7) Алгебраическая модель шифра гаммирования.
- 8) Криптографическая стойкость шифра. Виды атак.
- 9) Практическая стойкость шифра.
- 10) Имитостойкость шифра.
- 11) Помехозащищенность шифра.
- 12) Методы криптоанализа.
- 13) Блочные шифры. Принципы построения.
- 14) Блочные шифры. DES. Функция шифрования, S-блоки.
- 15) Блочные шифры. ГОСТ 28147.
- 16) Блочные шифры. AES.
- 17) Блочные шифры. ГОСТ 34.12-2015
- 18) Режимы использования блочных шифров. ECB
- 19) Режимы использования блочных шифров. CBC
- 20) Режимы использования блочных шифров. OFB
- 21) Режимы использования блочных шифров. CFB.
- 22) Комбинирование блочных шифров
- 23) Поточные шифры. Синхронные и самосинхронизирующиеся шифры
- 24) Поточные шифры. Принципы построения. Связь с режимами блочных шифров.

- 25) Поточные шифры. RC4.
- 26) Датчики истинно случайных последовательностей. Требования. Источники. Свойства.
- 27) Генераторы псевдослучайной последовательности. Методы усложнения.
- 28) Методы тестирования случайных последовательностей.
- 29) Понятие односторонней функции и функции с секретом.
- 30) Схемы шифрования с открытым ключом.
- 31) Схема шифрования RSA.
- 32) Схема шифрования Эль-Гамала.
- 33) Электронная подпись. Основные понятия.
- 34) Конструкция электронной подписи на основе односторонней функции с секретом
- 35) Конструкция электронной подписи на основе схемы шифрования с открытым ключом
- 36) Схема электронной подписи RSA
- 37) Схема электронной подписи ГОСТ Р 3410-2012
- 38) Криптографические хэш-функции. Основные понятия.
- 39) Хэш-функция по ГОСТ Р 3411-94 и ГОСТ Р 3411-2012.
- 40) Варианты применения хэш-функций.
- 41) Коды аутентификации сообщений. Определение, применение.
- 42) Типовые конструкции кодов аутентификации сообщений.
- 43) Вычисление имитовставки ГОСТ Р 28147
- 44) Криптографические протоколы. Протоколы аутентификации.
- 45) Криптографические протоколы. Протоколы распределения ключей. Схема Диффи-Хеллмана.
- 46) Управление ключами. Классификация ключей и угрозы управлению ключами.
- 47) Управление ключами. Процедуры управления ключами.
- 48) Инфраструктура открытых ключей. Варианты построения.
- 49) Инфраструктура открытых ключей. Назначение и основные функции удостоверяющего центра.
- 50) Сертификаты открытых ключей. Формат сертификата открытого ключа согласно X.509.
- 51) Положение о разработке СКЗИ

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) Методы и средства криптографической защиты информации
Код, специальность 10.05.03 Информационная безопасность автоматизированных систем
Специализация Безопасность открытых информационных систем
Кафедра ИБ Курс 4 Семестр 8
Форма обучения – очная

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1.

1..... Криптографическая стойкость шифра. Виды атак

1) 2..... Хэш-функция по ГОСТ Р 3411-94 и ГОСТ Р 3411-2012.

Экзаменатор.....Качаева Г.И.

Утвержден на заседании кафедры (протокол №__ от _____ 20__ г.)

Зав. кафедрой (название)Качаева Г.И.

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).