Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

Кафедра «Программного обеспечения вычислительной техники и автоматизированных систем»

**ОДОБРЕНО**

**Методической комиссией по укрупненной группе специальностей и направлений 10.00.00 «Информационная безопасность»**
**Председатель МК:**

_____ **Мелехин В.Б.**
Подпись ФИО

«17» 10 2018 г.

**УТВЕРЖДАЮ:**

**Декан, председатель совета факультета КТВТиЭ,**

_____ **Юсуфов Ш.А.**
Подпись
ФИО

«18» 10 2018г.

# Фонд оценочных средств

по дисциплине «Информационная безопасность открытых систем» для контроля знаний обучающихся направления подготовки 10.05.03 «Информационная безопасность автоматизированных». Специализация «Безопасность открытых информационных систем».

Составитель _____ Качаева Г.И.

Фонд оценочных средств обсужден на заседании кафедры «Информационная безопасность» «15» 10 2018г., протокол № 2

Зав. кафедрой _____ Качаева Г.И.

Фонд оценочных средств является приложением к рабочей программе по дисциплине С1.Б.34 - «Информационная безопасность открытых систем».

Махачкала, 2018 г.

**Оглавление**

## 1. Перечень компетенций с указанием этапов их формирования в процессе освоения ООП

### 1.1. Перечень компетенций и планируемые результаты

Табл.1

| № | Содержание и код компетенций по ФГОС | В результате изучения дисциплины «Информационная безопасность открытых систем» обучающиеся должны: | | |
|---|---|---|---|---|
| | | знать | уметь | владеть |
| 1 | способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ПК-4) | средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации | пользоваться нормативными документами по противодействию технической разведке | методами и средствами технической защиты информации |
| 2 | способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-5) | организацию защиты информации от утечки по техническим каналам на объектах информатизации | оценивать качество готового программного обеспечения | методами расчета и инструментального контроля показателей технической защиты информации |
| 3 | способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11) | подходы к интеграции сетей в открытых информационных системах | проектировать защищенные открытые информационные системы | терминологией и системным подходом построения защищенных открытых информационных систем |
| 4 | способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12) | принципы работы сетевых протоколов и технологий передачи данных в открытых информационных системах | определять и устранять основные угрозы информационной безопасности для открытых информационных систем | навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах |
| 5 | способностью участвовать в | основные методы и средства реализа- | строить модель нарушителя информа- | навыками анализа угроз и навы- |

| | | | | |
|---|---|---|---|---|
| | проектировании средств защиты информации автоматизированной системы (ПК-13) | ции удаленных сетевых атак на открытые информационные системы | ционной безопасности для открытых информационных систем | ками построения политик безопасности для открытых информационных систем виртуальных сетей. |
| 6 | способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19) | о политиках безопасности и мерах защиты в открытых информационных системах | выявлять и устранять уязвимости в основных компонентах открытых информационных систем | терминологией и системным подходом построения защищенных открытых информационных систем |
| 7 | способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20) | о комплексном подходе к построению эшелонированной защиты для открытых информационных систем систем | применять стандартные решения для защиты информации в открытых информационных системах и квалифицированно оценивать их качество | навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах |
| 8 | способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21) | о политиках безопасности и мерах защиты в открытых информационных системах | использовать современные методы и средства, разрабатывать и оценивать модели и политику безопасности для открытых информационных систем | навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем виртуальных сетей. |
| 9 | способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22) | о комплексном подходе к построению эшелонированной защиты для открытых информационных систем систем | выявлять и устранять уязвимости в основных компонентах открытых информационных систем | навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах |

### 1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Информационная безопасность открытых систем» определяется на следующих трех этапах:

1. Этап текущих аттестаций (вх.контр., текущие аттестации 1-3: СРС)
2. Этап промежуточных аттестаций (экзамен)

**Таблица 2**

| Код компетенций по ФГОС | Этапы формирования компетенций по дисциплине «Информационная безопасность открытых систем» | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | СЕМЕСТРЫ | | | | | | | | |
| | I | II | III -VI | VII | | | | | VIII-X |
| | - | - | - | Этап текущих аттестаций | | | | Этап промеж.аттест. | - |
| | - | - | - | 1 нед. | 2-5нед. | 6-10 нед. | 11-15нед. | 1-17 нед. | 18-20нед. | - |
| | - | - | - | Входной контроль | Текущая аттест.1 (контр.раб. 1) | Текущая аттест.2 (контр.раб.2) | Текущая аттест.3 (контр.раб.3) | СРС | Промеж.аттест. | - |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 11 | 12 |
| ПК-4 | - | - | - | + | + | + | + | + | + | + |
| ПК-5 | - | - | - | + | + | + | + | + | + | + |
| ПК-11 | - | - | - | + | + | + | + | + | + | + |
| ПК-12 | - | - | - | + | + | + | + | + | + | + |
| ПК-13 | - | - | - | + | + | + | + | + | + | + |
| ПК-19 | - | - | - | + | + | + | + | + | + | + |
| ПК-20 | - | - | - | + | + | + | + | + | + | + |
| ПК-21 | - | - | - | + | + | + | + | + | + | + |
| ПК-22 | - | - | - | + | + | + | + | + | + | + |

СРС – самостоятельная работа студентов:КР– курсовая работа;Знак «+» соответствует формированию компетенции.

## 2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.

В рамках текущих аттестаций (таблица 2) оценка уровня сформированности компетенций проводится на занятиях:

- лекционного типа посредством экспресс-опроса обучаемых, в том числе по темам и разделам, вынесенных для самостоятельного изучения;
- лабораторного типа путем устного опроса выполненных лабораторных заданий;
- практического типа методами проведения письменных контрольных работ.

Оценка сформированности компетенций в рамках промежуточной аттестации проводится по билетам для зачета. Они включают в себя вопросы для оценки знаний, умений и навыков, т.е. задания:

- *репродуктивного уровня,* позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умения правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины;
- *реконструктивного уровня,* позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей;
- *творческого уровня,* позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.

В ходе проведения текущей и промежуточной аттестации оцениваются:

- полнота и содержательность ответа;
- умение привести примеры из области операционных систем;
- умение пользоваться дополнительной литературой и современными технологиями обучения при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций, учебной литературы, интернет- ресурсам и другим источникам информации.

В ходе проведения оценки сформированности компетенций рекомендуются применение современных компьютерных технологий и виртуальных форм опроса в интерактивном режиме.

## 2.1. Описание показателей оценивания компетенций

Таблица 3

| Оценка «неудовлетворительно» (не зачтено) или отсутствие сформированности компетенции | Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции | Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции | Оценка «отлично» (зачтено) или высокий уровень освоения компетенции |
|---|---|---|---|
| Неспособность обучаемого самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения. отсутствие самостоятельности в применении умения к использованию методов освоения учебной дисциплины и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу свидетельствуют об отсутствии сформированной компетенции. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения учебной дисциплины. Уровень освоения дисциплины, при котором у обучаемого не сформировано | Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне. При наличии более 50% сформированных компетенций по дисциплинам, имеющим возможность доформирования компетенций на последующих этапах обучения. Для дисциплин итогового формирования | Способность обучающегося продемонстрировать самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые представлял преподаватель при потенциальном формировании компетенции, подтверждает наличие сформированной компетенции, причем на более высоком уровне. Наличие сформированной компетенции на повышенном уровне самостоятельности со стороны обучаемого при ее практической демонстрации в ходе решения аналогичных заданий следует оценивать как положительное и устойчиво закрепленное в практическом навыке. Для определения уровня освоения промежуточной дисциплины на оценку «хорошо» обучающийся должен продемонстрировать наличие 80% сформированных | Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной дисциплины с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи. Оценка «отлично» по дисциплине с промежуточным освоением компетенций, может быть выставлена при 100% подтверждении наличия компетенций, либо при 90% |

| | | | |
|---|---|---|---|
| более 50% компетенций. Если же учебная дисциплина выступает в качестве итогового этапа формирования компетенций (чаще всего это дисциплины профессионального цикла) оценка «неудовлетворительно» должна быть выставлена при отсутствии сформированности хотя бы одной компетенции. | компетенций естественно выставлять оценку «удовлетворительно», если сформированы все компетенции и более 60% дисциплин профессионального цикла «удовлетворительно». | компетенций, из которых не менее 1/3 оценены отметкой «хорошо». Оценивание итоговой дисциплины на «хорошо» обуславливается наличием у обучаемого всех сформированных компетенций причем общепрофессиональных компетенции по учебной дисциплине должны быть сформированы не менее чем на 60% на повышенном уровне, то есть с оценкой «хорошо». | сформированных компетенций, из которых не менее 2/3 оценены отметкой «хорошо». В случае оценивания уровня освоения дисциплины с итоговым формированием компетенций оценка «отлично» может быть выставлена при подтверждении 100% наличия сформированной компетенции у обучаемого, выполнены требования к получению оценки «хорошо» и освоены на «отлично» не менее 50% общепрофессиональных компетенций. |

## 2.2. Описание критериев определения уровня сформированности компетенций

Таблица 4

| Уровнисформированности компетенций | Критерии определения уровня сформированности | Компеенции, формируемые в результате освоения дисциплины ООП | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Профессиональные компетенции (ПК) | | | | | | | |
| | | ПК-4 | ПК-5 | ПК-11 | ПК-12 | ПК-13 | ПК 19 | ПК-20 | ПК-21 | ПК-22 |
| Пороговый | Компетенция сформирована | | | | + | | | + | | |
| | Демонстрируется недостаточный уровень самостоятельности навыка | | | | | | | | | |
| | Обладаст качеством **репродукции** | | | | | | | | | |
| Достаточный | Компетенция сформирована | | | | + | | | + | | |
| | Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка | | | | | | | | | |
| | Обладает качеством **реконструкции** | | | | | | | | | |
| Высокий | Компетенция сформирована | | | | + | | | + | | |
| | Демонстрируется высокий уровень | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | самостоятельности, высокая адаптивность практического навыка | | | | | | | | | |
| | Обладает **творческим** качеством | | | | | | | | | |

## 2.3. Описание шкал оценивания

В Дагестанском государственном техническом университете внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

**Таблица 5**

| Шкалы оценивания | | | Критерии оценивания |
|---|---|---|---|
| пятибальная | двадцатибальная | стобальная | |
| «Отлично» - 5 баллов | «Отлично» - 18-20 баллов | «Отлично» - 85 баллов | Показывает высокий уровень сформированности компетенций, т.е.:<br>– продемонстрирует глубокое и прочное усвоение материала;<br>– исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал;<br>– правильно формирует определения;<br>– демонстрирует умения самостоятельной работы с нормативно-правовой литературой;<br>– умеет делать выводы по излагаемому материалу. |
| «Хорошо» - 4 баллов | «Хорошо» - 15 -17 баллов | «Хорошо» - 70-84 баллов | Показывает достаточный уровень сформированности компетенций, т.е.:<br>– демонстрирует достаточно полное знание материала, основных теоретических положений;<br>– достаточно последовательно, грамотно логически стройно излагает материал;<br>– демонстрирует умения ориентироваться в нормальной литературе;<br>– умеет делать достаточно обоснованные выводы по излагаемому материалу. |
| «Удовлетворительно» - 3 баллов | «Удовлетворительно» - 12-14 баллов | «Удовлетворительно» - 56-69баллов | Показывает пороговый уровень сформированности компетенций. т.е.:<br>– демонстрирует общее знание изучаемого материала;<br>– испытывает серьезные затруднения при ответах на дополнительные вопросы:<br>– знает основную рекомендуемую литературу;<br>– умеет строить ответ в соответствии со структурой излагаемого материала. |
| «Неудовлетворительно» - 2 баллов | «Неудовлетворительно» - 1-11 баллов | «Неудовлетворительно» - 1-55 баллов | Ставится в случае:<br>– незнания значительной части программного материала;<br>– невладения понятийным аппаратом дисциплины;<br>– допущения существенных ошибок при изложении учебного материала;<br>– неумение строить ответ в соответствии со структурой излагаемого вопроса;<br>– неумение делать выводы по излагаемому материалу. |

**2.4. Определение уровня сформированности компетенций в результате изучения дисциплины«Информационная безопасность открытых систем»**

**Таблица 6**

| № | Код компетенций по ФГОС | Уровни сформированности компетенций | | |
|---|---|---|---|---|
| | | **Пороговый** | **Достаточный** | **Высокий** |
| 1 | 2 | 3 | 4 | 5 |
| I | ОПК-7 | **Знает** средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации**(на пороговом уровне, или на « удовлетворительно»).** **Умеет** пользоваться нормативными документами по противодействию технической разведке**слабо.** **Владеет** методами и средствами технической защиты информации**слабо.** | **Знает** средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации**на достаточном уровне («на «хорошо»).** **Умеет** пользоваться нормативными документами по противодействию технической разведке**на достаточном уровне.** **Владеет** методами и средствами технической защиты информации**на достаточном уровне.** | **Знает** средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации**полноценно (на высоком уровне, на «отлично»).** **Умеет** пользоваться нормативными документами по противодействию технической разведке**полноценно.** **Владеет** методами и средствами технической защиты информации**полноценно.** |
| | ПК-1 | **Знает** организацию защиты информации от утечки по техническим каналам на объектах информатизации**(на пороговом уровне, или на « удовлетворительно»).** **Умеет** оценивать качество готового программного обеспечения**слабо.** | **Знает** организацию защиты информации от утечки по техническим каналам на объектах информатизации**на достаточном уровне («на «хорошо»).** **Умеет** оценивать качество готового программного обеспечения**на достаточном уровне.** | **Знает** организацию защиты информации от утечки по техническим каналам на объектах информатизации**полноценно (на высоком уровне, на «отлично»).** **Умеет** оценивать качество готового программного обеспечения**полноценно.** |

| | | | | |
|---|---|---|---|---|
| | | **Владеет** методами расчета и инструментального контроля показателей технической защиты информации**слабо.** | **Владеет** методами расчета и инструментального контроля показателей технической защиты информациина **достаточном уровне.** | **Владеет** методами расчета и инструментального контроля показателей технической защиты информации**полноценно.** |

## 3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения ООП.

### 3.1. Задания для входного контроля

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).

### 3.2 Вопросы для текущих контрольных работ

#### 3.2.1 Аттестационная контрольная работа №1

1. Стандартизация и модельное представление открытых информационных систем.
2. Роль стандартов в технологии открытых систем.
3. Основные группы стандартов и организации по стандартизации.
4. Модель OSI и POSIX. Интранет как открытая система.
5. Разработка и управление Политикой использования ресурсов интранета.
6. Уязвимость открытых систем на примере интранета
7. Анализ угроз ИБ ресурсам интранета и причины их реализации.
8. Уязвимости операционных систем, серверов, рабочих станций, каналов связи.
9. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, WorldWideWeb.
10. Команды удаленного выполнения, Sendmail и электронная почта. Атаки на открытые системы
11. Атаки на открытые системы: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети.
12. Этапы реализации и уровни атак.
13. Атаки с использованием сетевых протоколов.
14. Обеспечение информационной безопасности в открытых системах.
15. Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408.
16. Разработка Политики безопасности для открытых систем.
17. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление.

#### 3.2.2 Аттестационная контрольная работа №2

1. Анализ угроз ИБ ресурсам интранета и причины их реализации.
2. Уязвимости операционных систем, серверов, рабочих станций, каналов связи.
3. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, WorldWideWeb.
4. Команды удаленного выполнения, Sendmail и электронная почта. Атаки на открытые системы
5. Атаки на открытые системы: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети.
6. Этапы реализации и уровни атак.

7. Атаки с использованием сетевых протоколов.

### 3.3.3 Аттестационная контрольная работа №3

1. Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408.
2. Разработка Политики безопасности для открытых систем.
3. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление.
4. Аутентификация субъектов и объектов взаимодействия в открытых системах.
5. Построение единых систем аутентификации, авторизации, персонализации, делегированного управления данными о субъектах и объектах и аудита доступа. Анализ типовой модели аутентификации.
6. Виртуальные вычислительные сети.
7. Виды ВЧВС в зависимости от решаемых задач: Intranet VPN, Client/server VPN, Extranet VPN, RemoteAccess VPN.

## 3.3 Перечень вопросов на экзамен

1. Стандартизация и модельное представление открытых информационных систем.
2. Роль стандартов в технологии открытых систем.
3. Основные группы стандартов и организации по стандартизации.
4. Модель OSI и POSIX. Интранет как открытая система.
5. Разработка и управление Политикой использования ресурсов интранета.
6. Уязвимость открытых систем на примере интранета
7. Анализ угроз ИБ ресурсам интранета и причины их реализации.
8. Уязвимости операционных систем, серверов, рабочих станций, каналов связи.
9. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, WorldWideWeb,
10. Команды удаленного выполнения, Sendmail и электронная почта. Атаки на открытые системы
11. Атаки на открытые системы: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети.
12. Этапы реализации и уровни атак.
13. Атаки с использованием сетевых протоколов.
14. Обеспечение информационной безопасности в открытых системах.
15. Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408.
16. Разработка Политики безопасности для открытых систем.
17. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление.
18. Аутентификация субъектов и объектов взаимодействия в открытых системах.
19. Построение единых систем аутентификации, авторизации, персонализации, делегированного управления данными о субъектах и объектах и аудита доступа. Анализ типовой модели аутентификации.
20. Виртуальные вычислительные сети.
21. Виды ВЧВС в зависимости от решаемых задач: Intranet VPN, Client/server VPN, Extranet VPN, RemoteAccess VPN.
22. Тема 8. Межсетевые экраны.
23. Системы анализа защищенности. Системы обнаружения и предотвращения вторжений.

24. Типы межсетевых экранов: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, межсетевые экраны экспертного уровня, персональные межсетевые экраны. Сетевой сканер XSpider. Система обнаружения вторжений Cisco IPS.

### 3.4 Вопросы для проверки остаточных знаний по дисциплине «Информационная безопасность открытых систем»

1. Этапы реализации и уровни атак.
2. Атаки с использованием сетевых протоколов.
3. Обеспечение информационной безопасности в открытых системах.
4. Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408.
5. Разработка Политики безопасности для открытых систем.
6. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление.

## 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

В качестве методического материала рекомендуется использовать:

1. Положение о ФОС в ФГБОУ ВО «Дагестанский государственный технический университет» (Приложение № 9 к ООП).
2. Положение ФГБОУ ВО «Дагестанский государственный технический университет» о модульно-рейтинговой системе оценки учебной деятельности студентов.
3. Процедура проведения оценочных мероприятий.

### 4.1. Процедура проведения оценочных мероприятий

**4.1.1. Текущий контроль**представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля (текущей аттестации) можно отнести устный опрос, письменные задания, контрольные работы.

Основные этапы текущего контроля:

– в конце каждой лекции или лабораторного занятия студентам выдаются задания для внеаудиторного выполнения по соответствующей теме;

– срок выполнения задания устанавливается по расписанию занятий (к очередной лекции или лабораторному занятию);

– студентам, пропускающим занятия, выдаются дополнительные задания – представить конспект пропущенного занятия, написанный «от руки» с последующим собеседованием по теме занятия;

– подведение итогов контроля проводится по графику проведения текущего контроля;

– результаты оценки успеваемости заносятся в рейтинговую ведомость и доводятся до сведения студентов;

К достоинствам данного типа относится его систематичность, непосредственно коррелирующаяся с требованием постоянного и непрерывного мониторинга качества обучения, а также возможность бально-рейтинговой оценки успеваемости обучающихся.

Недостатком является фрагментарность и локальность проверки. Компетенцию целиком, а не отдельные ее элементы (знания, умения, навыки) при подобном контроле проверить невозможно.

**4.1.2.Промежуточная аттестация**, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов).

Промежуточная аттестация помогает оценить более крупные совокупности знаний и умений, в некоторых случаях – даже формирование определенных профессиональных компетенций.

Достоинства: помогает оценить более крупные совокупности знаний и умений, в некоторых случаях – даже формирование определенных профессиональных компетенций.

Форма промежуточной аттестации: **экзамен**.

Текущий контроль и промежуточная аттестация традиционно служат основным средством обеспечения в учебном процессе «обратной связи» между преподавателем и обучающимся, необходимой для стимулирования работы обучающихся и совершенствования методики преподавания учебных дисциплин.

Основные этапы промежуточной аттестации:

- экзамен проводится по расписанию сессии;
- форма проведения занятия – письменная контрольная работа;
- вид контроля – фронтальный;
- требование к содержанию контрольной работы – дать краткий ответ на поставленный вопрос (задание);
- количество вопросов в билете;
- итоговая оценка определяется как сумма оценок, полученных в текущей аттестации и по результатам написания контрольной работы;
- проверка ответов и объявление результатов производится в день написания контрольной работы;
- результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента (при получении экзамена).

Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

При первой попытке ликвидации задолженности, во время зачетной недели или в течение сессии, студенту выдаются все задания по текущему контролю и промежуточной аттестации, по которым он не смог набрать зачетное количество баллов.