

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»  
(СПбГУТ)**

---

Кафедра Защищенных систем связи  
(полное наименование кафедры)

УТВЕРЖДЕН  
на заседании кафедры № 10 от 17.06.2020

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ**

---

Криптографические методы защиты информации  
(наименование дисциплины)

---

12.03.03 Фотоника и оптоинформатика  
(код и наименование направления подготовки / специальности)

---

Фотоника в инфокоммуникациях  
(направленность / профиль образовательной программы)

Санкт-Петербург

## **1. Общие положения**

Фонд оценочных средств (ФОС) по дисциплине используется в целях нормирования процедуры оценивания качества подготовки и осуществляет установление соответствия учебных достижений запланированным результатам обучения и требованиям образовательной программы дисциплины.

Предметом оценивания являются знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций у обучающихся.

Процедуры оценивания применяются в процессе обучения на каждом этапе формирования компетенций посредством определения для отдельных составных частей дисциплины методов контроля – оценочных средств.

Основным механизмом оценки качества подготовки и формой контроля учебной работы студентов являются текущий контроль успеваемости и промежуточная аттестация. Общие требования к процедурам проведения текущего контроля и промежуточной аттестации определяет внутренний локальный акт университета: Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся. При проведении текущего контроля успеваемости и промежуточной аттестации студентов используется ФОС.

### **1.1. Цель и задачи текущего контроля студентов по дисциплине.**

Цель текущего контроля – систематическая проверка степени освоения программы дисциплины «Криптографические методы защиты информации», уровня достижения планируемых результатов обучения - знаний, умений, навыков, в ходе ее изучения при проведении занятий, предусмотренных учебным планом.

Задачи текущего контроля:

1. обнаружение и устранение пробелов в освоении учебной дисциплины;
2. своевременное выполнение корректирующих действий по содержанию и организации процесса обучения;
3. определение индивидуального учебного рейтинга студентов;
4. подготовка к промежуточной аттестации.

В течение семестра при изучении дисциплины реализуется традиционная система поэтапного оценивания уровня освоения. За каждый вид учебных действий студенты получают оценку .

### **1.2. Цель и задачи промежуточной аттестации студентов по дисциплине.**

Цель промежуточной аттестации – проверка степени усвоения студентами учебного материала, уровня достижения планируемых результатов обучения и сформированности компетенций на момент завершения изучения дисциплины.

Промежуточная аттестация проходит в форме экзамена.

Задачи промежуточной аттестации:

1. определение уровня освоения учебной дисциплины;
2. определение уровня достижения планируемых результатов обучения и сформированности компетенций;
3. соотнесение планируемых результатов обучения с планируемыми результатами освоения образовательной программы в рамках изученной дисциплины.

## 2. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

### 2.1.Перечень компетенций.

**ОПК-4** Способен использовать современные информационные технологии и программное обеспечение при решении задач профессиональной деятельности, соблюдая требования информационной безопасности

### 2.2.Этапы формирования компетенций.

Таблица 1

| Код компетенции | Этап формирования компетенции  | Вид учебной работы  | Тип контроля  | Форма контроля   |
|-----------------|--------------------------------|---|---------------|------------------|
| ОПК-4           | теоретический (информационный) | лекции, самостоятельная работа                              | текущий       | собеседование    |
|                 | практико-ориентированный       | практические (лабораторные) занятия, самостоятельная работа | текущий       | домашнее задание |
|                 | оценочный                      | аттестация  | промежуточный | экзамен          |

Применяемые образовательные технологии определяются видом контактной работы.

### 2.3.Соответствие разделов дисциплины формируемым компетенциям.

Этапами формирования компетенций являются взаимосвязанная логическая последовательность освоения разделов (тем) учебной дисциплины.

Таблица 2

| № п/п | Раздел (тема) дисциплины   | Содержание раздела (темы) дисциплины   | Коды компетенций |
|-------|--|--|------------------|
| 1     | Раздел 1.<br>Методы и средства криптографии в инфокоммуникациях                    | История криптографии. Основные понятия и определения. Требования к криптографическим системам. Исторические шифры. Современные методы и средства криптографии.   | ОПК-4            |
| 2     | Раздел 2.<br>Симметричные криптографические системы , использующие блоковые шифры. | Основные классы симметричных крипtosистем. Общие сведения о блочных шифрах . Примеры алгоритмов блочного шифрования.:DES и его модификации, AES( Rijndael), . RC5.,Российский стандарт ГОСТ28147-89 . Режимы использования блочных шифров. Многократное шифрование | ОПК-4            |
| 3     | Раздел 3.<br>Симметричные криптографические системы использующие потоковые шифры.  | Особенности потоковых шифров. Свойства линейного рекуррентного регистра. Нелинейные узлы усложнения. Примеры алгоритмов потокового шифрования :RC4, A5/1.  | ОПК-4            |

|   |   |  |       |
|---|---|--|-------|
| 4 | Раздел 4.<br>Симметричные криптографические системы использующие потоковые шифры.                       | Классификации систем аутентификации и характеристики их эффективности. Безусловно стойкие системы аутентификации. Вычислительно стойкие системы аутентификации. Использование модификаций блоковых шифров. Примеры систем аутентификаций , использующих блоковые шифры (ГОСТ28147 и др.)   | ОПК-4 |
| 5 | Раздел 5.<br>Основные принципы построения несимметричных криптосистем (криптосистем с открытым ключом). | Основные требования , предъявляемые к криптосистемам с открытым ключом. Основы теории чисел и теории конечных полей. Свойства эллиптических кривых.  | ОПК-4 |
| 6 | Раздел 6.<br>Примеры построения криптосистем с открытым ключом  | Криптосистемы : РША , Рабина, Эль-Гамаля, Диффи-Хеллмана , Мак-Элис. Построение криптосистем на основе теории эллиптических кривых. Использование сертификатов.  | ОПК-4 |
| 7 | Раздел 7.<br>Электронные (цифровые подписи) и криптографические протоколы..                             | Принцип построения цифровых подписей (ЦП) на основе использования криптосистем с открытым ключом. Определение и свойства криптографических хеш-функций. Примеры построения ЦП :DSA, ГОСТ Р 3410-94. Понятие о криптографических протоколах. Примеры криптографических протоколов : разделение секретов , идентификация , совместные вычисления , тайное голосование. Методы формирования и распределения аутентифицированных ключей. | ОПК-4 |

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

#### **3.1.Описание показателей оценивания компетенций на различных этапах их формирования.**

Таблица 3

| Код компетенции | Показатели оценивания (индикаторы достижения компетенций)   | Оценочные средства  |
|-----------------|---|---|
| ОПК-4           | ОПК-4.1 Использует современные информационные технологии и программное обеспечение при решении задач профессиональной деятельности;<br>ОПК-4.2 Соблюдает требования информационной безопасности при использовании современных информационных технологий и программного обеспечения; | ТЕОРЕТИЧЕСКИЙ ЭТАП: собеседование<br>ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: домашнее задание<br>ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену |

#### **3.2.Стандартные критерии оценивания.**

Критерии разработаны с учетом требований ФГОС ВО к конечным результатам обучения и создают основу для выявления уровня сформированности компетенций: минимального, базового или высокого.

### **Критерии оценки устного ответа в ходе собеседования:**

- логика при изложении содержания ответа на вопрос, выявленные знания соответствуют объему и глубине их раскрытия в источнике;
- использование научной терминологии в контексте ответа;
- объяснение причинно-следственных и функциональных связей;
- умение оценивать действия субъектов социальной жизни, формулировать собственные суждения и аргументы по определенным проблемам;
- эмоциональное богатство речи, образное и яркое выражение мыслей.

### **Критерии оценки ответа за экзамен:**

Для экзамена в устном виде употребимы критерии оценки устного ответа в ходе собеседования (см. выше)

### **Критерии оценки лабораторной работы:**

- Выполнение лабораторной работы (подготовленность к выполнению, осознание цели работы, методов созиания схемы, проведение измерений и фиксирования их результатов, приложение, самостоятельность выполнения, наличие и правильность оформления необходимых материалов для проведения работы – схема соединений, таблицы записей и т.п.);
- Оформление отчета по лабораторной работе (аккуратность оформления результатов измерений, правильность вычислений, правильность выполнения графиков, векторных диаграмм и др.) ;
- Правильность и самостоятельность выбора формул для расчетов при оформлении результатов работы;
- Правильность построения графиков, умение объяснить их характер;
- Правильность построения векторных диаграмм, умение их строить и понимание того, что они значат;
- Ответы на контрольные вопросы к лабораторной работе.

### **Общие критерии оценки работы студента на практических занятиях:**

- Отлично - активное участие в обсуждении проблем каждого семинара, самостоятельность ответов, свободное владение материалом, полные и аргументированные ответы на вопросы семинара, участие в дискуссиях, твёрдое знание лекционного материала, обязательной и рекомендованной дополнительной литературы, регулярная посещаемость занятий.
- Хорошо - недостаточно полное раскрытие некоторых вопросов темы, незначительные ошибки в формулировке категорий и понятий, меньшая активность на семинарах, неполное знание дополнительной литературы, хорошая посещаемостью
- Удовлетворительно - ответы отражают в целом понимание темы, знание содержания основных категорий и понятий, знакомство с лекционным материалом и рекомендованной основной литературой, недостаточная активность на занятиях, оставляющая желать лучшего посещаемость.
- Неудовлетворительно - пассивность на семинарах, частая неготовность при ответах на вопросы, плохая посещаемость, отсутствие качеств, указанных выше для получения более высоких оценок.

Порядок применения критерииев оценки конкретизирован ниже, в разделе 4,

содержащем оценочные средства для текущего контроля успеваемости и для проведения промежуточной аттестации студентов по данной дисциплине.

### **3.3.Описание шкал оценивания.**

В процессе оценивания результатов обучения и компетенций на различных этапах их формирования при освоении дисциплины для всех перечисленных выше оценочных средств используется шкала оценивания, приведенная в таблице .

Дихотомическая шкала оценивания используется при проведении текущего контроля успеваемости студентов: при проведении собеседования, при приеме эссе, реферата, а также может быть использована в целях проведения такой формы промежуточной аттестации, как зачет (шкала приводится для всех оценочных средств из таблицы 3.

Таблица 4

| <b>Показатели оценивания</b>   | <b>Описание в соответствии с критериями оценивания</b>                                    | <b>Оценка знаний, умений, навыков и опыта</b>      | <b>Оценка по бальной шкале</b> |
|--------------------------------|---|--|--------------------------------|
| Высокий уровень освоения       | Демонстрирует полное понимание проблемы. Требования по всем критериям выполнены           | «очень высокая», «высокая»                         | «отлично»                      |
| Базовый уровень освоения       | Демонстрирует значительное понимание проблемы. Требования по всем критериям выполнены     | «достаточно высокая», «выше средней», «базовая»    | «хорошо»                       |
| Минимальный уровень освоения   | Демонстрирует частичное понимание проблемы. Требования по большинству критериев выполнены | «средняя», «ниже средней», «низкая», «минимальная» | «удовлетворительно»            |
| Недостаточный уровень освоения | Демонстрирует небольшое понимание проблемы. Требования по многим критериям не выполнены   | «очень низкая», «примитивная»                      | «неудовлетворительно»          |

При проведении промежуточной аттестации студентов по данной дисциплине в форме экзамена используется пятибалльная шкала оценивания.

## **4. Типовые контрольные задания, иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

### **4.1.Оценочные средства промежуточной аттестации**

Оценочные средства промежуточной аттестации по дисциплине представлены в Приложении 1.

### **4.2.Формирование тестового задания промежуточной аттестации**

#### **Аттестация №1**

В экзаменационном билете присутствует 2 вопроса теоретической направленности. Теоретические вопросы позволяют оценить уровень знаний и

частично – умений.

Примерный перечень заданий, выносимых на промежуточную аттестацию, разрешенных учебных и наглядных пособий, средств материально-технического обеспечения :

#### **По вопросу 1, компетенции ОПК-4**

- 1 Модель шифрования - расшифрования дискретных сообщений.
- 2 Необходимое условие построения ТНДШ систем.
- 3 Понятие расстояния единственности.
- 4 Потоковые шифры Методы формирования шифрующей последовательности. ЛРР (использование в потоковых шифрах).
- 5 Атака на потоковый шифр при неизменной гамме.
- 6 Свойства потоковых шифров и примеры использования. Построение потокового шифра на основе блокового.
- 7 Многократное шифрование. Свойства. Особенности использования.
- 8 Модифицированные алгоритмы блокового шифрования.
- 9 Параметры наиболее известных блоковых шифров.
- 10 Методы формирования блоковых шифров на основе SP сетей.
- 11 Основные типы преобразований при построении блоковых шифров.
- 12 Проблемы оценки стойкости современных криптосистем.
- 13 Достаточное условия построения ТНДШ систем.
- 14 Принципы построения асимметричных криптосистем.
- 15 Способы реализации преобразований в блоковых шифрах. Структура Файстеля. Примеры использования.
- 16 Атака со вставкой на потоковый шифр.
- 17 Дополнительные криптографические протоколы. Обеспечение безопасности взаимодействия пользователей.
- 18 Модульная арифметика (нахождение обратного элемента по модулю, функция Эйлера, малая теорема Ферма, тесты на простоту).
- 19 Управление ключами. Понятие мастер ключа и сессионных ключей. Способы хранения ключей.
- 20 Модификации с обратной связью по криптограмме и по выходу.
- 21 Цифровая подпись. Алгоритмы реализации цифровой подписи. Стандарты цифровой подписи.
- 22 Особенности обмена ключами в симметричной и асимметричной системе шифрования (гибридная система шифрования).
- 23 Потенциальные атаки на RSA. Нахождение секретного ключа, слабые прости числа.
- 24 Модульная арифметика (понятие о модульной арифметике, сложение, умножение, возведение в степень, логарифмирование, факторизация, НОД).
- 25 Потоковые шифры (методы построения, свойства, примеры).
- 26 Стандарты блокового шифрования.
- 27 Принципы построения блоковых шифров.
- 28 Криптосистема Эль-Гамаля. Сравнение симметричных и асимметричных криптосистем. (Свойства асимметричных криптосистем).
- 29 Понятие хеш функции. Применение в цифровой подписи. Требования к хеш-функции.
- 30 Способы определения расстояния единственности. Примеры.

#### **По вопросу 2, компетенции ОПК-4**

- 1 Определить расстояние единственности для криптограммы сообщения с энтропией равной 1,5, если шифрование выполнено российским стандартом шифрования AES.

Определить достаточное число ключей для реализации алгоритма ТНДШ для

2 возможности шифрования 10 сообщений, если в каждом сообщении может быть до 100 двоичных символов.

Определить расстояние единственности для криптограммы сообщения с энтропией

3 равной 2, если шифрование выполнено российским стандартом шифрования ГОСТ 28147-89.

Определить расстояние единственности для криптограммы сообщения с энтропией

4 равной 2,5, если шифрование выполнено российским стандартом шифрования ГОСТ Р 34.12-2015

5 Определить количество ключей в системе шифрования методом простой замены для текста на английском языке.

6 Вычислить функцию Эйлера для следующих аргументов: 323, 1013, 10403.

7 Определить верхнюю границу эффективного объёма ключа при двухкратном шифровании на разных ключах на алгоритме DES.

8 Определить среднее количество коллизий при использовании хеширования с длиной хеша 10 бит для сообщений длиной 22 бита.

Определить расстояние единственности для криптограммы сообщения с энтропией

9 равной 2,5, если шифрование выполнено российским стандартом шифрования ГОСТ Р 34.12-2015

10 Определить количество единиц на периоде выходной последовательности ЛРР заданного следующим полиномом:  $h(x)=x^4+x+1$ .

11 Произвести шифрования сообщения по алгоритму РША. Вычислить криптограмму из сообщения  $M=3$ . Открытый ключ:  $K=5$ ,  $N=187$ .

12 Определить количество ключей в системе шифрования методом простой замены для текста на английском языке.

13 Выполнить пошагово тест Миллера для числа 561 по основанию 2.

14 Найти значения следующих выражений:  $2^{12} \bmod 11$ ,  $2^{22} \bmod 35$ ,  $4*3^{(-1)} \bmod 5$ .

15 Выполнить пошагово алгоритм разложения на множители Ферма для числа 253.

16 Определить количество необходимое количество шагов для выполнения алгоритма разложения на множители методом проб.

17 Выполнить по шагам вычисление  $3^8 \bmod 7$  быстрым алгоритмом возведения в степень.

Определить итоговый ключ в алгоритме Диффи-Хелмана, если заданы открытые

18 параметры  $a=3$  и модуль преобразований  $p=31$ , секретные числа пользователей  $A$  и  $B$  составляют 5 и 7 соответственно.

19 Найти секретный ключ для алгоритма РША, если открытый ключ:  $K=7$ ,  $N=24$ .

20 Найти все возможные значения модуля шифрования меньшие 20.

21 Сформировать цифровую подпись для сообщения  $M=7$ , если используется алгоритм РША (без хеширования). Секретный ключ пользователя:  $k=3$ ,  $N=77$ .

22 Выполнить пошагово алгоритм разложения на множители Ферма для числа 253.

23 Выполнить по шагам вычисление  $2^{11} \bmod 7$  быстрым алгоритмом возведения в степень.

Определить итоговый ключ в алгоритме Диффи-Хелмана, если заданы открытые

24 параметры  $a=3$  и модуль преобразований  $p=31$ , секретные числа пользователей  $A$  и  $B$  составляют 5 и 7 соответственно.

25 Найти секретный ключ для алгоритма РША, если открытый ключ:  $K=7$ ,  $N=20$ .

26 Выполнить пошагово алгоритм Эвклида для аргументов 1234 и 54.

27 Выполнить пошагово тест Миллера для числа 25 по основанию 7.

28 Определить количество единиц на периоде выходной последовательности ЛРР заданного следующим полиномом:  $h(x)=x^5+x+1$ .

29 Определить достаточное число ключей для реализации алгоритма ТНДШ для возможности шифрования 5 сообщений, если в каждом сообщении может быть до 200 двоичных символов.

30 Оценить сверху максимально возможный объём подписанного сообщения, если в качестве алгоритма цифровой подписи используется алгоритм Эль-Гамаля (без хеширования и без разбиения сообщения на блоки) с параметрами:  $a=31$ ,  $p=9901$ .

Представленный по каждому вопросу перечень заданий является рабочей моделью для генерирования экзаменационных билетов.

#### 4.3.Развернутые критерии выставления оценки

Таблица 5

| Тип вопроса             | Показатели оценки  |  |  |  |
|-------------------------|--|--|--|--|
|                         | 5  | 4  | 3  | 2  |
| Теоретические вопросы   | тема разносторонне проанализирована, ответ полный, ошибок нет, предложены обоснованные аргументы и приведены примеры эффективности аналогичных решений | тема разносторонне раскрыта, ответ полный, допущено не более 1 ошибки, предложены обоснованные аргументы и приведены примеры эффективности аналогичных решений | тема освещена поверхностно, ответ полный, допущено более 2 ошибок, обоснованных аргументов не предложено | ответы на вопрос билета практически не даны  |
| Практические вопросы    | задание выполнено без ошибок, студент может дать все необходимые пояснения, сделать выводы   | задание выполнено без ошибок, но студент не может пояснить ход выполнения и сделать необходимые выводы   | задание выполнено с одной ошибкой, при ответе на вопрос ошибка замечена и исправлена самостоятельно      | задание невыполнено или выполнено с двумя и более ошибками, пояснения к ходу выполнения недостаточны |
| Дополнительные вопросы  | ответы даны на все вопросы, показан творческий подход  | ответы даны на все вопросы, творческий подход отсутствует  | ответы на дополнительные вопросы ошибочны (2 и более ошибок)   | ответы на дополнительные вопросы практически отсутствуют   |
| <b>Уровень освоения</b> | высокий  | базовый  | минимальный  | недостаточный  |

Для получения оценки «отлично» студент должен показать высокий уровень освоения всех компетенций, предусмотренных программой данной дисциплины, оценки «хорошо» - базовый, оценки «удовлетворительно» - минимальный. В случае разноранговых оценок определения уровня освоения каждой из компетенций, общая оценка знаний по дисциплине детерминируется как:

- Отлично, - если ответ на практический вопрос и более половины всех ответов на вопросы, включая дополнительные, оценены на «5», остальные – на «4»
- Хорошо, - более половины ответов оценены на «4», остальные – на «5»; либо ответ на один теоретический вопрос оценен на «3», остальные – на «4» и «5»
- Удовлетворительно, - если два и более ответов на вопросы билета оценены на «3», и ни один из ответов не определен как «2»
- Неудовлетворительно, - если ответ на один из вопросов оценен на «2»

#### **4.4.Комплект экзаменационных билетов**

Комплект экзаменационных билетов ежегодно обновляется и формируется перед экзаменом.

Развернутые критерии выставления оценки за экзамен содержатся в таблице 5.

### **5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и/или опыта деятельности, характеризующих этапы формирования компетенций**

#### **5.1.Методические материалы для текущего контроля успеваемости**

Текущий контроль предусматривает систематическое оценивание процесса обучения, с учетом необходимости обеспечения достижения обучающимися планируемых результатов обучения по дисциплине (уровня сформированности знаний, умений, навыков, компетенций), а также степени готовности обучающихся к профессиональной деятельности. Система текущего контроля успеваемости и промежуточной аттестации студентов предусматривает решение следующих задач:

- оценка качества освоения студентами основной профессиональной образовательной программы;
- аттестация студентов на соответствие их персональных достижений поэтапным требованиям соответствующей основной профессиональной образовательной программы;
- поддержание постоянной обратной связи и принятие оптимальных решений в управлении качеством обучения студентов на уровне преподавателя, кафедры, факультета и университета.

В начале учебного изучения дисциплины преподаватель проводит входной контроль знаний студентов, приобретённых на предшествующем этапе обучения.

#### **Задания, реализуемые только при проведении текущего контроля**

**Собеседование** - это средство контроля, организованное как специальная беседа преподавателя со студентом на темы, связанные с изучаемой дисциплиной, и рассчитанное на выявление объема знаний студента по определенному разделу, теме, проблеме и т.п., соответствующих освоению компетенций, предусмотренных рабочей программой дисциплины.

Проблематика, выносимая на собеседование, определяется преподавателем в заданиях для самостоятельной работы студента, а также на семинарских и практических занятиях. В ходе собеседования студент должен уметь обсудить с преподавателем соответствующую проблематику на уровне диалога и показать

установленный уровень владения компетенциями.

## **5.2.Методические материалы для промежуточной аттестации**

Форма промежуточной аттестации по дисциплине – экзамен

Форма проведения экзамена: устная

В аудиторию, где принимается экзамен, приглашаются студенты из расчета не более пяти экзаменующихся на одного экзаменатора.

Хорошо успевающим студентам, выполнившим все виды работ, предусмотренные рабочей программой дисциплины и не имеющим задолженности, деканатом факультета может быть разрешена сдача экзаменов досрочно с согласия экзаменатора, без освобождения студентов от текущих учебных занятий. Досрочная сдача экзаменов проводится не ранее, чем за 1 месяц до начала сессии. В период сессии досрочная сдача не разрешается. Решение о досрочной сдаче принимает декан факультета на основе личного заявления студента, согласованного с преподавателями дисциплин, выносимых на сессию.

Для подготовки к ответу на экзамену студенту рекомендуется использовать Перечень теоретических вопросов (заданий), выносимых на экзамен, разрешенных учебных и наглядных пособий, средств материально-технического обеспечения и типовые практические задания (задачи), перечисленных в п.4.2.

В экзаменационный билет входит теоретических вопроса: один – из минимального уровня, – из базового и одно практическое задание, характеризующее высокий уровень сформированности компетенций. Время подготовки ответа при сдаче в устной форме должно составлять не менее 40 минут (по желанию обучающегося ответ может быть досрочным). Время ответа – не более 15 минут.

Экзаменатору предоставляется право задавать обучающимся дополнительные вопросы в рамках программы дисциплины текущего семестра, а также, помимо теоретических вопросов, давать задачи, которые изучались на практических занятиях.

Основой для определения оценки служит уровень усвоения студентами материала, предусмотренного рабочей программой дисциплины. Знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций у обучающихся, определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» или «зачтено», «незачтено».

Выбор формы оценивания определяется целями и задачами обучения. В числе применяемых форм оценивания выделяют интегральную и дифференцируемую оценку, а также самоанализ и самоконтроль студента. Источники информации, которые используются при применении разных форм оценивания:

- работы обучающихся: домашние задания, презентации, отчеты, дневники, эссе и т.п.;
- результаты индивидуальной и совместной деятельности студентов в процессе обучения;
- результаты выполнения контрольных работ, тестов;
- другие источники информации.

Для того чтобы оценка выполняла те функции, которые на нее возложены как на характеристику этапов формирования компетенций у обучающихся, необходимо

соблюдение следующих базовых принципов оценивания:

- непрерывность процесса оценивания;
- оценивание должно быть критериальным, основанным на целях обучения;
- критерии выставления оценки и алгоритм ее выставления должны быть заранее известны;
- включение обучающихся в контрольно-оценочную деятельность.

Конечный результат обучения (с точки зрения соответствия его заявленным целям) в высокой степени определяется набором критериальных показателей, которые используются в процессе оценки.

Студенту, использующему в ходе экзамена неразрешенные источники и средства для получения информации, выставляется неудовлетворительная оценка. В случае неявки студента на экзамен, преподавателем делается в экзаменационной ведомости отметка «не явился». Пересдача экзамена в целях повышения положительной оценки не допускается.