

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

Средства криптографической защиты информации
_____ (наименование дисциплины)

11.05.04 Инфокоммуникационные технологии и системы
специальной связи
_____ (код и наименование направления подготовки /специальности/)

Системы коммутации и сети связи специального назначения
_____ (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 «Средства криптографической 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 Способность понимать сущность и значение информации в развитии современного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности

ОПК-6 Способность использовать основные методы, способы и средства получения, хранения, обработки и защиты информации

ПК-8 Способность организовывать и осуществлять выполнение мероприятий по защите государственной тайны и безопасности информации

2.2. Этапы формирования компетенций.

Таблица 1

Код компетенции	Этап формирования компетенции	Вид учебной работы	Тип контроля	Форма контроля
ОПК-4, ОПК-6, ПК-8	теоретический (информационный)	лекции, самостоятельная работа	текущий	собеседование
	практико-ориентированный	практические (лабораторные) занятия, самостоятельная работа	текущий	контрольная работа
	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. Принципы построения систем шифрования	Введение в криптографию. Типы криптосистем. Модель системы шифрования. Способы шифрования. Влияние ошибок в криптограмме на дешифрование.	ОПК-4
2	Раздел 2. Безусловностойкие криптосистемы	Необходимые и достаточные условия построения безусловно стойких криптосистем. Понятие расстояния единственности. Вывод формулы для расстояния единственности для произвольного шифра и ее анализ.	ОПК-4
3	Раздел 3. Блочные шифры	Принципы построения блочных шифров. Шифры на основе схемы Фейстеля. Подстановочно перестановочные шифры. Методы криптоанализа блочных шифров: тотальный перебор ключей, анализ статистики криптограммы, линейный и дифференциальный. Модификации блочных шифров. Стандарты шифрования AES, ГОСТ 34.12-15.	ОПК-6

4	Раздел 4. Потоковые шифры	Принципы построения потоковых шифров. Линейный рекуррентный регистр и его свойства. Нелинейные узлы усложнения, используемые для построения потоковых шифров. Нерегулярное тактирование в потоковых шифрах. Основные методы криптоанализа потоковых шифров. Анализ шифра А5 стандарта GSM.	ОПК-6
5	Раздел 5. Аутентификация сообщений	Модель системы аутентификации, классификация, характеристики эффективности. Безусловно стойкие системы аутентификации. Вычислительно-стойкие системы аутентификации. Способы построения ключевых хэш-функций. Системы аутентификации, на основе блочного шифра.	ПК-8
6	Раздел 6. Управление ключами в симметричных криптосистемах	Модель управления ключами. Этапы жизненного цикла ключа. Распределение ключей на основе ЦРК и доверенных каналов. Распределение ключей в интерактивном режиме с использованием ЦРК.	ПК-8

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, критерии оценивания (планируемые результаты обучения)	Оценочные средства
ОПК-4	ЗНАЕТ: сущность и значение информации в развитии современного общества; УМЕЕТ: определять опасности и угрозы, возникающие в этом процессе; ВЛАДЕЕТ: навыками в выполнении требований информационной безопасности;	ТЕОРЕТИЧЕСКИЙ ЭТАП: собеседование ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: контрольная работа ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену
ОПК-6	ЗНАЕТ: способы и средства получения, хранения, обработки и защиты информации; УМЕЕТ: использовать основные методы, способы и средства получения, хранения, обработки и защиты информации; ВЛАДЕЕТ: основными методами и способами хранения, обработки и защиты информации;	ТЕОРЕТИЧЕСКИЙ ЭТАП: собеседование ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: контрольная работа ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену
ПК-8	ЗНАЕТ: основы организации мероприятий по защите государственной тайны и безопасности информации; УМЕЕТ: организовывать и осуществлять выполнение мероприятий по защите государственной тайны и безопасности информации; ВЛАДЕЕТ: компьютерными программами защиты информации, например, как поставить пароль, как зашифровать файл и т.д.;	ТЕОРЕТИЧЕСКИЙ ЭТАП: собеседование ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: контрольная работа 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 употребляемы критерии оценки устного ответа в ходе собеседования (см. выше)

Критерии оценки контрольной работы:

- работа была выполнена автором самостоятельно;
- студент подобрал достаточный список литературы, которая необходима для осмысления темы контрольной;
- автор сумел составить логически обоснованный план, который соответствует поставленным задачам и сформулированной цели;
- студент анализирует материал;
- контрольная работа отвечает всем требованиям четкости изложения и аргументированности, объективности и логичности, грамотности и корректности;
- студент сумел обосновать свою точку зрения;
- контрольная работа соответствует всем требованиям по оформлению;
- автор защитил контрольную и успешно ответил на все вопросы преподавателя.

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 критериев 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

Показатели оценивания	Описание в соответствии с критериями оценивания	Оценка знаний, умений, навыков и опыта	Оценка по бальной шкале
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 и практической направленности. Теоретические вопросы позволяют оценить уровень знаний и частично - умений, практические - уровень умений и владения

компетенцией.

Примерный перечень заданий, выносимых на промежуточную аттестацию, разрешенных учебных и наглядных пособий, средств материально-технического обеспечения и типовые практические задания (задачи):

По вопросу 1, компетенции ОПК-4, ПК-8

- 1 Методы распределения ключей на основе физических особенностей канала связи.
- 2 Атака со вставкой на потоковый шифр.
- 3 Проблемы оценки стойкости современных криптосистем.
- 4 Методы формирования блочных шифров на основе SP сетей.
- 5 Потенциальные атаки на RSA. Нахождение секретного ключа, слабые просты числа.
- 6 Понятие хеш функции. Применение в цифровой подписи. Требования к хеш-функции.
- 7 Понятие аутентификации. Аутентификация сообщений. Аутентификация пользователей.
- 8 Потоковые шифры (методы построения, свойства, примеры).
- 9 Особенности обмена ключами в симметричной и асимметричной системе шифрования (гибридная система шифрования).
- 10 Описание криптосистемы RSA. Сложность операций в RSA.
- 11 Модификация с зацеплением блоков.
- 12 Модульная арифметика (нахождение обратного элемента по модулю, функция Эйлера, малая теорема Ферма, тесты на простоту).
- 13 Цифровая подпись. Алгоритмы реализации цифровой подписи. Стандарты цифровой подписи.
- 14 Параметры наиболее известных блочных шифров.
- 15 Модульная арифметика (понятие о модульной арифметике, сложение, умножение, возведение в степень, логарифмирование, факторизация, НОД).
- 16 Модификации с обратной связью по криптограмме и по выходу.
- 17 Модификация в виде электронной кодовой книги.
- 18 Криптосистема Эль-Гамала. Сравнение симметричных и асимметричных криптосистем. (Свойства асимметричных криптосистем).
- 19 Принципы построения асимметричных криптосистем.
- 20 Основные типы преобразований при построении блочных шифров.
- 21 Атака на потоковый шифр при неизменной гамме.
- 22 Модифицированные алгоритмы блочного шифрования.
- 23 Способы реализации преобразований в блочных шифрах. Структура Файстеля. Примеры использования.
- 24 Многократное шифрование. Свойства. Особенности использования.
- 25 Стандарты блочного шифрования.
- 26 Принципы построения блочных шифров.
- 27 Свойства потоковых шифров и примеры использования. Построение потокового шифра на основе блочного.
- 28 Потоковые шифры Методы формирования шифрующей последовательности. ЛРР (использование в потоковых шифрах).
- 29 Сведения из теории сложности. Понятие о простых и сложных алгоритмах.
- 30 Способы определения расстояния единственности. Примеры.

По вопросу 2, компетенции ОПК-6

- 1 Выполнить пошагово алгоритм разложения на множители Ферма для числа 253.
- 2 Произвести шифрование сообщения по алгоритму RSA. Вычислить криптограмму из сообщения $M=3$. Открытый ключ: $K=5$, $N=187$.

- 3 Определить количество единиц на периоде выходной последовательности ЛПРР заданного следующим полиномом: $h(x)=x^5+x+1$.
- 4 Определить верхнюю границу эффективного объёма ключа при двухкратном шифровании на разных ключах на алгоритме DES.
- 5 Определить количество ключей в системе шифрования методом простой замены для текста на английском языке.
- 6 Произвести шифрования сообщения по алгоритму РША. Вычислить криптограмму из сообщения $M=3$. Открытый ключ: $K=5$, $N=187$.
- 7 Выполнить пошагово алгоритм Эвклида для аргументов 1234 и 54.
Определить достаточное число ключей для реализации алгоритма ТНДШ для
- 8 возможности шифрования 10 сообщений, если в каждом сообщении может быть до 100 двоичных символов.
Определить достаточное число ключей для реализации алгоритма ТНДШ для
- 9 возможности шифрования 5 сообщений, если в каждом сообщении может быть до 200 двоичных символов.
- 10 Выполнить пошагово тест Миллера для числа 561 по основанию 2.
- 11 Выполнить по шагам вычисление $3^8 \bmod 7$ быстрым алгоритмом возведения в степень.
Определить итоговый ключ в алгоритме Диффи-Хелмана, если заданы открытые
- 12 параметры $a=3$ и модуль преобразований $p=31$, секретные числа пользователей А и В составляют 5 и 7 соответственно.
- 13 Найти секретный ключ для алгоритма РША, если открытый ключ: $K=7$, $N=20$.
- 14 Найти значения следующих выражений: $2^{12} \bmod 11$, $2^{22} \bmod 35$, $4 \cdot 3^{(-1)} \bmod 5$.
- 15 Определить количество необходимое количество шагов для выполнения алгоритма разложения на множители методом проб.
- 16 Вычислить функцию Эйлера для следующих аргументов: 323, 1013, 10403.
- 17 Определить расстояние единственности для криптограммы сообщения с энтропией равной 1,5, если шифрование выполнено российским стандартом шифрования AES.
- 18 Сформировать цифровую подпись для сообщения $M=7$, если используется алгоритм РША (без хеширования). Секретный ключ пользователя: $k=3$, $N=77$.
- 19 Определить среднее количество коллизий при использовании хеширования с длиной хеша 10 бит для сообщений длиной 22 бита.
- 20 Найти секретный ключ для алгоритма РША, если открытый ключ: $K=7$, $N=24$.
- 21 Найти все возможные значения модуля шифрования меньше 20.
- 22 Выполнить пошагово тест Миллера для числа 25 по основанию 7.
- 23 Определить количество единиц на периоде выходной последовательности ЛПРР заданного следующим полиномом: $h(x)=x^4+x+1$.
- 24 Вычислить функцию Эйлера для следующих аргументов: 323, 1013, 10403.
- 25 Найти значения следующих выражений: $3^{10} \bmod 11$, $3^{24} \bmod 35$, $4 \cdot 2^{(-1)} \bmod 5$.
Оценить сверху максимально возможный объём подписанного сообщения, если в
- 26 качестве алгоритма цифровой подписи используется алгоритм Эль-Гамала (без хеширования и без разбиения сообщения на блоки) с параметрами: $a=31$, $p=9901$.
- 27 Определить количество единиц на периоде выходной последовательности ЛПРР заданного следующим полиномом: $h(x)=x^4+x+1$.
Определить расстояние единственности для криптограммы сообщения с энтропией
- 28 равной 2, если шифрование выполнено российским стандартом шифрования ГОСТ 28147-89.
Определить расстояние единственности для криптограммы сообщения с энтропией
- 29 равной 2,5, если шифрование выполнено российским стандартом шифрования ГОСТ Р 34.12-2015
- 30 Выполнить по шагам вычисление $2^{11} \bmod 7$ быстрым алгоритмом возведения в степень.

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 рассмотрена со всех сторон, проанализирована, ответ полный, ошибок нет, предложены обоснованные аргументы и приведены примеры эффективности аналогичных решений	тема рассмотрена со всех сторон, 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	задача решена без ошибок, студент может дать все необходимые пояснения к решению, сделать выводы	задача решена без ошибок, но студент не может пояснить ход решения и сделать необходимые выводы	задача решена с одной ошибкой, при ответе на вопрос ошибка замечена и исправлена самостоятельно	задача не решена или решена с двумя и более ошибками, пояснения к ходу решения 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
Уровень освоения	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 усвоенный уровень владения компетенциями.

5.2.Методические материалы для промежуточной аттестации

Форма промежуточной аттестации по дисциплине - экзамен

Форма проведения экзамена: смешанная

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 экзамене 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.