Приложение А

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)

10.05.02 Информационная безопасность телекоммуникационных систем
(код и наименование направления подготовки / специальности)

Безопасность телекоммуникационных систем информационного взаимодействия
(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-2 способностью применять соответствующий математический аппарат для решения профессиональных задач

ПК-1 способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем

2.2.Этапы формирования компетенций.

Таблица 1

Код компетенции	Этап формирования компетенции	Вид учебной работы	Тип контроля	Форма контроля
ОПК-2, ПК-1	теоретический (информационный)	лекции, самостоятельная работа	текущий	собеседование, реферат, тест
	практико-ориентированный	практические (лабораторные) занятия, самостоятельная работа	текущий	реферат, тест
	оценочный	аттестация	промежу-точный	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. Методы и средства криптографии в инфокоммуникациях	История криптографии. Основные понятия и определения. Требования к криптографическим системам. Исторические шифры. Современные методы и средства криптографии.	ОПК-2
2	Раздел 2. Симметричные криптографические системы , использующие блоковые шифры.	Основные классы симметричных криптосистем. 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-2
3	Раздел 3. Симметричные криптографические системы использующие потоковые шифры.	Особенности потоковых шифров. Свойства линейного рекуррентного регистра. Нелинейные узлы усложнения. Примеры алгоритмов потокового шифрования :RC4, A5/1.	ОПК-2

4	Раздел 4. Аутентификация сообщений с использованием симметричных криптографических систем.	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.)	ПК-1
5	Раздел 5. 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.	ПК-1
6	Раздел 6. Примеры построения криптосистем с открытым ключом.	Криптосистемы : РША , Рабина, Эль-Гамаля, Диффи-Хеллмана , Мак-Элис. Построение криптосистем на основе теории эллиптических кривых. Использование сертификатов.	ПК-1
7	Раздел 7. Электронные (цифровые подписи) и криптографические протоколы..	Принцип построения цифровых подписей (ЦП) на основе использования криптосистем с открытым ключом. Определение и свойства криптографическиххещ-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.	ПК-1

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 компе-тенции	Показатели, критерии оценивания (планируемые результаты обучения)	Оценочные средства
ОПК-2	ЗНАЕТ: Способы организации и поддержки комплекса мер по информационной безопасности, управления процессом их реализации; УМЕЕТ: Программно реализовать алгоритмы безопасности; ВЛАДЕЕТ: Методами организации защиты объекта от внешних угроз и технологиями защиты информации;	ТЕОРЕТИЧЕСКИЙ ЭТАП: собеседование, реферат ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: реферат ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену

ПК-1	ЗНАЕТ: Способы организации и поддержки комплекса мер по информационной безопасности, управления процессом их реализации; УМЕЕТ: Программно реализовать алгоритмы безопасности; ВЛАДЕЕТ: Методами организации защиты объекта от внешних угроз и технологиями защиты информации;	ТЕОРЕТИЧЕСКИЙ ЭТАП: собеседование, тест ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: тест 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 реферата:

- содержание раскрывает тему;
- логичность изложения материала при раскрытии темы, наличие выводов;
- оформление реферата соответствует установленным требованиям;
- реферат автором был представлен с использованием демонстрационного материала;
- качество выступления автора: свободное владение материалом; текст зачитывает; кратко и точно отвечает на вопросы и т.д.;
- результаты проверки текста реферата на оригинальность составили не менее 60%.

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 собирания схемы, проведение измерений и фиксирования их результатов, прилежание, 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.

Критерии оценки тестового контроля знаний:

студентом даны правильные ответы на
- 91-100% заданий - отлично,
- 81-90% заданий - хорошо,
- 71-80% заданий - удовлетворительно,
- 70% заданий и менее – неудовлетворительно.

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»	«удовлетво-рительно»
Недостаточный уровень освоения	Демонстрирует небольшое понимание проблемы. Требования по многим критериям не выполнены	«очень низкая», «примитивная»	«неудовлетво-рительно»

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-2

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 просты 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 ПК-1

1 Определить расстояние единственности для криптограммы сообщения с энтропией равной 1,5, если шифрование выполнено российским стандартом шифрования AES.
2 Определить достаточное число ключей для реализации алгоритма ТНДШ для возможности шифрования 10 сообщений, если в каждом сообщении может быть до 100 двоичных символов.
3 Определить расстояние единственности для криптограммы сообщения с энтропией равной 2, если шифрование выполнено российским стандартом шифрования ГОСТ 28147-89.
4 Определить расстояние единственности для криптограммы сообщения с энтропией 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.
9 Определить расстояние единственности для криптограммы сообщения с энтропией 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 mod11, 2^22 mod35, 4*3^(-1)mod5.

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 mod 7 быстрым алгоритмом возведения в степень.

18 Определить итоговый ключ в алгоритме Диффи-Хелмана, если заданы открытые 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 mod 7 быстрым алгоритмом возведения в степень.

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

Теорети-ческие 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
Практи-ческие 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
Дополни-тельные 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	недоста-точный

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

Реферат – это разновидность самостоятельной учебно-исследовательской работы студента, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

Цель написания реферата состоит в закреплении имеющихся у студентов навыков самостоятельной работы. В процессе работы над рефератом студент получает дополнительную возможность проявления своих творческих способностей, что находит выражение в таком представлении материала, которое позволит развить умение популярно излагать сложные вопросы и применить системный подход для последующего обобщения полученных результатов.

Структура и содержание реферата определяется целью выполнения работы. Если основной целью является углубленное изучение какого-либо вопроса или темы изучаемой дисциплины, то работу можно свести к краткому изложению реферируемой научной работы, книги или статьи. Если же реферирование производится для того, чтобы подготовить доклад на заданную тему, то имеет место критический обзор литературы и других источников.

Работа студента над рефератом состоит из следующих этапов:

- выбор темы на основе перечня, разработанного кафедрой;
- уяснение актуальности данной темы, цели и задач, которые необходимо решить;
- составление предварительного плана работы по теме реферата;
- накопление и подготовка информационного материала;
- обобщение материала и написание реферата;

- оформление в соответствии с требованиями, предъявляемыми к такого рода работам;
- защита реферата на семинаре или конференции.

Содержание материала должно быть логичным, его изложение носит проблемно-поисковый характер. Студент вправе избрать для реферата, доклада любую тему в пределах программы изучаемой учебной дисциплины. Важно при этом учитывать ее актуальность, научную разработанность, возможность нахождения необходимых источников для изучения темы реферата, доклада, имеющиеся у студента начальные знания и личный интерес к выбору данной темы. Реферат, доклад должен отражать: знание современного состояния проблемы; обоснование выбранной темы; использование известных результатов и фактов; полноту цитируемой литературы, ссылки на работы ученых, занимающихся данной проблемой; актуальность поставленной проблемы; материал, подтверждающий научное, либо практическое значение в настоящее время. Рекомендуемый объем реферата 10-15 страниц компьютерного (машинописного) текста, доклада - 2-3 страницы.

В основе работы над выполнением реферата лежит предварительный план, который состоит обычно из трех-четырех вопросов, а в процессе работы он уточняется и конкретизируется. План определяет структуру, содержание и логическую взаимосвязь частей. При составлении предварительного плана работы по теме, в основной части реферата особое внимание следует уделить глубокому теоретическому освещению как темы в целом, так и отдельных ее вопросов, правильно увязать теоретические положения с практикой, конкретным фактическим и цифровым материалом. Целесообразно предварительно намеченный план согласовать на консультации с преподавателем кафедры, ведущим семинарские занятия или читающим лекционный курс. План не следует излишне детализировать, в нем перечисляются основные, центральные вопросы темы в логической последовательности. Главы можно не разбивать на параграфы.

Структура реферата:

1. Титульный лист (оформляется по шаблону)

2. Введение (содержит: актуальность, цель, задачи, которые необходимо решить для достижения поставленной цели).

3. Основная часть (детализируется в соответствии с планом реферата)

- Теоретические основы рассматриваемого процесса, принципа, явления, функции, опыта и т.д. (О чем идет речь?)
- Проблемы практической реализации рассматриваемого процесса, принципа, явления, функции, опыта и т.д. (В чем суть проблемы?)

4. Заключение

- Краткое изложение (аннотация) полученных результатов раскрытия изучаемой темы
- Собственное отношение к описанной проблеме (Что Вы думаете по существу темы и что предлагаете?)

5. Список использованных источников

6. Приложения

В содержании с указанием номеров страниц перечисляются такие составляющие реферата, как, введение, основная часть, заключение, список использованных источников и приложения (если они присутствуют).

Актуальность темы реферата определяется востребованностью информации по данному вопросу в обществе в целом, и – в научных кругах, в частности. Цель выполнения реферативной работы ставит перед студентом преподаватель во время выдачи индивидуального задания. Задачи, которые должны быть решены для достижения данной цели, студент формулирует самостоятельно. На основе этого формируется предварительный план работы по теме. Во введении помимо актуальности рассматриваемой проблемы, целей и задач, следует отметить, в каких произведениях известных ученых рассматривается изучаемая проблема.

Накопление и подготовка информационного материала – в зависимости от основной цели – охватывает как истоки, с которых началось изучение данного вопроса, так и современные представления и концепции. На данном этапе необходимо обращать внимание на современные источники информации со сроком давности за последние 3 года и указывать на их использование в списке источников информации.

Существенную помощь в ознакомлении с библиографией могут оказать библиотечные каталоги (алфавитный, систематический, предметный), библиографические указатели (учетно-регистрационные, научно-вспомогательные, рекомендательные, критические), справочная литература (энциклопедии, словари, предметные указатели в трудах отдельных ученых-экономистов). Определенную помощь могут оказать различные библиографические пособия по отдельным отраслям знаний, выпускаемые специальными центрами информации. Кроме того, крупнейшие библиотеки страны, такие как Российская национальная библиотека, Государственная национальная библиотека, выпускают рекомендательные библиографические указатели.

Реферат должен быть написан ясным языком, без повторений, сокращений, противоречий между отдельными положениями. Приводимые в тексте цитаты из научной литературы, а также статистические данные должны быть снабжены соответствующими ссылками на источники информации, из которых они взяты, с указанием автора, названия работы, издательства, года издания, тома, страницы. В перечень использованных источников и Интернет-ресурсов не могут быть включены рефераты, прочие готовые студенческие работы, а также ссылки на сайты рефератов, шпаргалок и прочее.

В заключении приводятся основные выводы и прочие обобщения, сделанные в ходе работы над рефератом.

Список использованных источников содержит перечень источников информации, на которые были сделаны ссылки в ходе выполнения работы. Перечень должен содержать не менее пяти источников.

Приложения, в отличие от всего остального, не являются обязательной составляющей реферата. В приложения могут быть вынесены материалы, помещение которых по тексту нецелесообразно по каким-либо причинам: они могут быть слишком объемны, могут иметь промежуточный характер, могут быть неудобны

для восприятия по тексту и т.д.

Работа над рефератом:

При работе над рефератом необходимо внимательно изучить соответствующую теме литературу, включая монографии, статистические сборники, материалы, публикуемые в научных журналах. Источниками фактического материала могут служить статистические сборники, газеты, журналы.

Особое внимание нужно обратить на использование Интернет-ресурсов. Существует великое многообразие электронных источников информации. Ссылки на эти источники допустимы лишь при условии, что студент указывает не только фамилию автора, название использованного материала и электронный адрес, по которому материал размещен, но и кем размещен данный материал, со ссылкой на ответственных за размещение.

Подготовленная информация конспектируется и/или систематизируется на электронном носителе в соответствии с предварительно намеченным планом. В процессе изучения материалов по теме реферата студент располагает материал в той последовательности, которая представляется ему наиболее стройной и целесообразной, фиксирует собственные мысли, которые он считает нужным изложить в тексте реферата. В этом случае происходит изменение предварительного плана реферата.

Необходимым требованием является представление материала в обобщенном виде. Студент обобщает накопленный и подготовленный материал и делает выводы, пользуясь системным подходом. Выводы, которые представляют обобщение важнейших положений, выдвинутых и рассмотренных в реферате, составляют значительную часть заключения.

Минимальные требования к оформлению реферата:

Материалы оформляются на листах формата А4 (297х210мм), односторонней печатью. Нумерация страниц: сквозная по всему документу, снизу от центра, арабскими цифрами, титульный лист включен в общую нумерацию страниц, но номер страницы на титульном листе не проставляется.

Поля текста: слева – 30 мм, справа – 10 мм, сверху и снизу – 20 мм. Размер абзацного отступа: 12,5 мм. Текст печатается шрифтом Times New Roman №12 или №14 с межстрочным интервалом 1,5. Выравнивание – по ширине.

Список использованной литературы оформляется в соответствии с ГОСТ 7.1-2003 «Библиографическая запись. Библиографическое описание».

Материалы должны быть представлены преподавателю в печатном и в электронном виде. Электронная версия реферата проходит проверку содержания на оригинальность и помещается в личное портфолио студента.

Не позднее, чем за 5 дней до защиты или выступления подготовленный реферат, доклад поступает на рецензирование преподавателю. Защита реферата или выступление с докладом продолжается в течение 5-7 минут по плану. Выступающему студенту по окончании представления реферата (доклада) могут быть заданы вопросы по теме реферата (доклада). В случае невыполнения доклада, реферата студенту необходимо принести письменный текст сообщения перед зачетом и получить его оценивание преподавателем. Общее количество набранных студентом баллов по дисциплине учитывается при проведении промежуточной

аттестации.

Студенты заочной формы обучения должны получить письменную рецензию преподавателя кафедры на представленный реферат, где дается общая оценка работы - «зачтено», «не зачтено» и указываются ее достоинства и недостатки.

Если реферат не зачитывается, то с учетом замечаний он должен быть переработан. Повторным рецензированием занимается тот преподаватель, который рецензировал реферат в первый раз.

Результаты работы над рефератом и его выполнения учитываются при проведении промежуточной аттестации.

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 установ ленный уровень владения компетенциями.

Тест – система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.

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 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.