

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 № 6 от 13.06.2018

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Управление информационной безопасностью
_____ (наименование дисциплины)

10.04.01 Информационная безопасность
_____ (код и наименование направления подготовки / специальности)

Безопасность компьютерных систем
_____ (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 «Управление информационной безопасностью», 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.

ОК-1 способностью к абстрактному мышлению, анализу, синтезу

ПК-1 способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты

ПК-13 способностью организовать управление информационной безопасностью

ПК-14 способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России

ПК-16 способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности

ПС-3 Формирование политик информационной безопасности

ПС-4 Разработка требований по защите компьютерных сетей и систем

ПС-7 Оценка рисков угроз и соответствия требованиям нормативных документов информационной безопасности

ПС-8 Проведение анализа безопасности компьютерных систем

2.2.Этапы формирования компетенций.

Таблица 1

Код компетенции	Этап формирования компетенции	Вид учебной работы	Тип контроля	Форма контроля
ОК-1, ПК-1, ПК-13, ПК-14, ПК-16, ПС-3, ПС-4, ПС-7, ПС-8	теоретический (информационный)	лекции, самостоятельная работа	текущий	
	практико-ориентированный	практические (лабораторные) занятия, самостоятельная работа	текущий	
	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. Управление информационной безопасностью на государственном уровне. Общие принципы и российская практика	Организационно-правовые формы управления безопасностью. Предпосылки развития государственного управления в сфере информационной безопасности. Общая методология и структура организационного обеспечения информационной безопасности на уровне государств. Общая политика России в сфере информационной безопасности. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.	
2	Раздел 2. Основные принципы построения SIEM	Средства визуализации элементов ИБ. Визуализация статистики по инцидентам ИБ. Комплексные системы мониторинга ИБ. Средства сбора отчетов и Logов. Основные принципы работы SIEM систем. Составление отчетов по ИБ.	
3	Раздел 3. Проведение комплекса процедур цифрового расследования в информационных и компьютерных системах	Digital Forensic. Расследование инцидентов. Утилиты для расследования инцидентов. Информация об истории посещения сайтов, кукисах, букмарках, скачанных файлах, заполненных формах, сохраненных логинах и т.д.	
4	Раздел 4. Введение в оценку и аудит ИБ путем выявления угроз ИБ «на лету»	Введение в «этический хакинг». Основные принципы его организации. Составление плана проведения тестирования целевой системы (инфраструктуры). Отношение к законодательству и регуляторам. Составление отчета и рекомендаций на основе проведенного тестирования.	
5	Раздел 5. Аудит систем удаленного и локального доступа	Основные механизмы и принципы проведения аудита ИБ СКУД предприятия, а также систем удаленного доступа с использованием технологий виртуальных частных сетей	
6	Раздел 6. Аудит инфраструктуры ИБ, интегрированных сервисов телефонии и беспроводного доступа	Основные механизмы и принципы проведения аудита ИБ инфраструктуры предприятия. Основные механизмы и принципы проведения аудита ИБ систем IP-телефонии, а также систем беспроводного доступа Wi-Fi	
7	Раздел 7. Принципы организации аудита систем информационной безопасности	Основные техники проведения аудита систем ИБ. Разработка методики проведения аудита систем ИБ. Основные средства проведения аудита систем ИБ.	

8	Раздел 8. Принципы построения интегрированных систем информационной безопасности	Создание политик ИБ предприятия. Принципы обеспечения безопасности инфраструктуры. Принципы обеспечения безопасности периметра сети телекоммуникационной системы. Регулирование правил работы СКУД. Регулирование правил удаленного доступа средствами VPN. Контроль безопасности конечных устройств. Контроль безопасности IP-телефонии.	
9	Раздел 9. Стандарты управления информационной безопасностью	Государственные стандарты в области ИБ РФ. Оценочные стандарты в информационной безопасности. Оранжевая книга. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования"	
10	Раздел 10. Оценка рисков информационной безопасности	Основные составляющие информационной безопасности. Угрозы информационной безопасности в информационных системах. Основные определения и критерии, угрозы целостности и конфиденциальности.	

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
ОК-1	ЗНАЕТ: произведение анализа, синтеза и абстрактного мышления УМЕЕТ: абстрактно мыслить, анализировать, синтезировать ВЛАДЕЕТ: способностью к абстрактному мышлению, анализу, синтезу	ТЕОРЕТИЧЕСКИЙ ЭТАП: ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: защита, ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену
ПК-1	ЗНАЕТ: основные методики оценки уровня информационной безопасности организации и примеры их использования УМЕЕТ: работать с основными программами, позволяющими реализовывать аудит систем ИБ и - работать с государственными и международными стандартами, регулирующих деятельность ВЛАДЕЕТ: способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ТЕОРЕТИЧЕСКИЙ ЭТАП: ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: защита, ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену

ПК-13	<p>ЗНАЕТ: организацию управления ИБ</p> <p>УМЕЕТ: производить организацию по управлению ИБ</p> <p>ВЛАДЕЕТ: способностью организовать управление информационной безопасностью</p>	<p>ТЕОРЕТИЧЕСКИЙ ЭТАП: ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП:защита, ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену</p>
ПК-14	<p>ЗНАЕТ: принципы работы с большими данными, основные понятия, касающиеся технологий обеспечения информационной безопасности больших данных</p> <p>УМЕЕТ: организовывать работу по созданию или модернизации систем и средств обеспечения ИБ в соответствии с правовыми нормами</p> <p>ВЛАДЕЕТ: способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России</p>	<p>ТЕОРЕТИЧЕСКИЙ ЭТАП: ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП:защита, ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену</p>
ПК-16	<p>ЗНАЕТ: разработку проектов, бизнес-планов, технической и эксплуатационной документации на системы, средства обеспечения ИБ</p> <p>УМЕЕТ: разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения ИБ</p> <p>ВЛАДЕЕТ: способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности</p>	<p>ТЕОРЕТИЧЕСКИЙ ЭТАП: ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП:защита, ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену</p>
ПС-3	<p>ЗНАЕТ: Формирование политик информационной безопасности</p> <p>УМЕЕТ: разрабатывать нормы и политики ИБ</p> <p>ВЛАДЕЕТ: умением формировать и создавать политики ИБ</p>	<p>ТЕОРЕТИЧЕСКИЙ ЭТАП: ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП:защита, ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену</p>
ПС-4	<p>ЗНАЕТ: разработку требований по защите компьютерных сетей и систем</p> <p>УМЕЕТ: разрабатывать требования по защите компьютерных сетей и систем</p> <p>ВЛАДЕЕТ: разработкой требований по защите компьютерных сетей и систем</p>	<p>ТЕОРЕТИЧЕСКИЙ ЭТАП: ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП:защита, ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену</p>
ПС-7	<p>ЗНАЕТ: как производить оценку рисков угроз, а также проверять соответствия требованиям нормативных документов ИБ</p> <p>УМЕЕТ: давать оценку рискам угроз и оценивать соответствия требованиям нормативных документов ИБ</p> <p>ВЛАДЕЕТ: оценкой рисков угроз и соответствия требованиям нормативных документов информационной безопасности</p>	<p>ТЕОРЕТИЧЕСКИЙ ЭТАП: ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП:защита, ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену</p>

ПС-8	ЗНАЕТ: актуальную и полную информацию по проведению анализа безопасности компьютерных систем УМЕЕТ: Анализировать безопасность компьютерных систем ВЛАДЕЕТ: навыками проведения аудита безопасности информационных систем	ТЕОРЕТИЧЕСКИЙ ЭТАП: ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: защита, ОЦЕНОЧНЫЙ ЭТАП: билеты к экзамену
------	---	--

Критерии, указанные в таблице 3, разработаны с учетом требований ФГОС ВО к конечным результатам обучения и создают основу для выявления уровня сформированности компетенций: минимального, базового или высокого.

3.2. Стандартные критерии оценивания.

Критерии оценки ответа за экзамен:

Для экзамена в устном виде :

- 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 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.

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, приведенными в таблице 3	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 текущего контроля успеваемости

Оценочные средства текущего контроля успеваемости 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 ОК-1

- 1 Основные составляющие информационной безопасности
- 2 Основные определения и критерии, угрозы целостности и конфиденциальности
- 3 Оценочные стандарты в информационной безопасности
- 4 Международный стандарт ISO/IEC 15408
- 5 Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения
- 6 Создание политик ИБ предприятия
- 7 Принципы обеспечения безопасности периметра сети телекоммуникационной системы
- 8 Регулирование правил удаленного доступа средствами VPN
- 9 Контроль безопасности IP-телефонии
- 10 Разработка методики проведения аудита систем ИБ
- 11 Основные механизмы и принципы проведения аудита ИБ инфраструктуры предприятия
- 12 Основные механизмы и принципы проведения аудита ИБ систем беспроводного доступа Wi-Fi
- 13 Основные механизмы и принципы проведения аудита ИБ систем удаленного доступа с использованием технологий виртуальных частных сетей
- 14 Основные принципы организации «этического хакинга»
- 15 Отношение «этического хакинга» к законодательству и регуляторам
- 16 DigitalForensic
- 17 Утилиты для расследования инцидентов
- 18 Средства визуализации элементов ИБ
- 19 Комплексные системы мониторинга ИБ
- 20 Основные принципы работы SIEM систем. Составление отчетов по ИБ
- 21 Структура понятия информационная безопасность
- 22 Организационное обеспечение ИБ
- 23 Компьютерные преступления и их классификация
- 24 Инженерно-техническое обеспечение компьютерной безопасности

- 25 Персональные данные и их защита
- 26 История компьютерных вирусов и современность
- 27 Почему плохо скачивать файлы с левого сайта
- 28 Кому нужна система защиты информации
- 29 Информационные угрозы для государства
- 30 Способы воздействия информационных угроз на объекты

По вопросу 2, компетенции ОК-1

- 1 Угрозы информационной безопасности в информационных системах
- 2 Государственные стандарты в области ИБ РФ
- 3 Оранжевая книга.
- 4 Критерии оценки безопасности информационных систем
- 5 Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасностью. Требования"
- 6 Принципы обеспечения безопасности инфраструктуры
- 7 Регулирование правил работы СКУД
- 8 Контроль безопасности конечных устройств
- 9 Основные техники проведения аудита систем ИБ
- 10 Основные средства проведения аудита систем ИБ
- 11 Основные механизмы и принципы проведения аудита ИБ систем IP-телефонии
- 12 Основные механизмы и принципы проведения аудита ИБ СКУД предприятия
- 13 Введение в «этический хакинг»
- 14 Составление плана проведения тестирования целевой системы (инфраструктуры)
- 15 Составление отчета и рекомендаций на основе проведенного тестирования.
- 16 Расследование инцидентов
- 17 Информация об истории посещения сайтов, кукисах, букмарках, скачанных файлах, заполненных формах, сохраненных логинах и т.д
- 18 Визуализация статистики по инцидентам ИБ
- 19 Оранжевая книга.
- 20 Организационно-правовые формы управления безопасностью
- 21 Защита информации в Интернете
- 22 Как предотвратить кражу личностей
- 23 Политика безопасности и ее принципы
- 24 Вредоносные программы, их виды
- 25 Методы и средства защиты информации
- 26 Система защиты информации и ее структура
- 27 Что такое Аутентификация
- 28 Организационно-правовой статус службы безопасности
- 29 Электронная почта и ее защита
- 30 Регулирование правил работы СКУД

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	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 установ

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 экзаменуемых 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.