ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

Б1.Б.1.25 Основы информационной безопасности

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов.

Квалификация выпускника специалист

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

ОК-5
Способностью понимать социальную значимость своей будущей профессии и. обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
Знать:
Этап 1: Цели, задачи, принципы и основные направления обеспечения информационной безопасности государства
Этап 2: Современные подходы к построению систем защиты информации
Уметь:
Этап 1:Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня защиты с учетом развития всех видов обеспечений вычислительных систем
Этап 2: Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.
Владеть:
Этап 1: Профессиональной терминологией и методами теоретического обоснования в выборе оптимальной концепции информационной безопасности
Этап 2: Владеть методологическими принципами оценки защищенности объектов информатизации и обеспечения требуемого уровня защиты

ОПК-5
Способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
Знать:
Этап 1: Знать основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики.
Этап 2: Знать принципы и методы разработки и применения систем обеспечения информации в научных исследованиях и в управлении технологическими, организационно-экономическими и социальными системами
Уметь:
Этап 1: Уметь взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности в научных исследованиях и проектно-конструкторской деятельности, а также в управлении технологическими, экономическими и социальными системами
Этап 2: Использовать полученные знания при реализации реальных проектов.
Владеть:
Этап 1: Навыки строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач.
Этап 2: Навыки пользования библиотеками прикладных программ для решения прикладных математических задач

ПК-4
Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

Знать:
Этап 1: Угрозы безопасности и методы защиты информации в банковских ин-формационных системах
Этап 2: Основные правила разработки политики безопасности организации. Компоненты политики безопасности
Уметь:
Этап 1: Выявлять угрозы системе информационной безопасности разрабатывать комплекс мер по ее совершенствованию
Этап 2: Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю
Владеть:
Этап 1: Оценки эффективности систем защиты информации автоматизированных систем
Этап 2: Навыки применения комплексного подхода к обеспечению информационной безопасности автоматизированных систем
ПК-5
Способностью проводить анализ рисков информационной безопасности автоматизированной системы
Знать:
Этап 1: Знать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления
ИБ
Этап 2: Знать цели и задачи, решаемые разрабатываемыми процессами управления ИБ
Уметь:
Этап 1 : Определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите
Этап 2: Оценивать информационные риски в автоматизированных системах
Владеть:
Этап 1: Навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности
Этап 2: Навыками и методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем, методы оценки информационных рисков

ПК-11
Способностью разрабатывать политику информационной безопасности автоматизированной системы
Знать:
Этап 1: Основные правила разработки политики организации. Компоненты политики безопасности
Этап 2: Принципы и методы противодействия несанкционированному информационному воздействию на информационные системы и системы передачи информации.
Уметь:
Этап 1: Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю;
Этап 2: Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

Владеть:

Этап 1: Внедрения политики безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю;
согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю
Этап 2: Навыки применения комплексного подхода к обеспечению информационной безопасности объекта защиты

ПК-22
Способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации
Знать:
Этап 1: Основные правила разработки политики безопасности организации. Компоненты политики безопасности
Этап 2: Принципы и методы противодействия несанкционированному информационному воздействию информационные системы
Уметь:
Этап 1 : Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю
Этап 2: Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.
Владеть:
Этап 1: Внедрения политики безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю;
согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю
Этап 2: Навыки применения комплексного
подхода к обеспечению информационной безопасности объекта защиты

2. Показатели и критерии оценивания компетенций на различных этапах их формирования.

Таблица 1 - Показатели и критерии оценивания компетенций на 1 этапе

Наименование компетенции	Критерии сформированности компетенции	Показатели	Процедура оценивания
1	2	3	4
ОК-5 Способностью понимать социальную значимость своей будущей профессии и. обладать высокой	Способен понимать социальную значимость своей будущей профессии и. обладание высокой мотивацией к	**Знания:** Цели, задачи, принципы и основные направления обеспечения информационной безопасности государства	Устный опрос

мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдение норм профессиональной этики	**Умения:** Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня защиты с учетом развития всех видов обеспечений вычислительных систем **Навыки:** Профессиональной терминологией и методами теоретического обоснования в выборе оптимальной концепции информационной безопасности	
ОПК-5 Способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Способен применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	**Знания:** Знать основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики. **Умения:** Уметь взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности в научных исследованиях и проектно-конструкторской деятельности, а также в управлении технологическими, экономическими и социальными системами **Навыки:** Навыки строить и изучать математические	Устный опрос

		модели конкретных явлений и процессов для решения расчетных и исследовательских задач.	
ПК-4 Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**Знания:** Угрозы безопасности и методы защиты информации в банковских ин-формационных системах **Умения:** Выявлять угрозы системе информационной безопасности разрабатывать комплекс мер по ее совершенствованию **Навыки:** Оценки эффективности систем защиты информации автоматизированных систем	Устный опрос
ПК-5 Способностью проводить анализ рисков информационной безопасности автоматизированной системы	Способен проводить анализ рисков информационной безопасности автоматизированной системы	**Знания:** Знать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ **Умения:** Определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите **Навыки:** Анализа информационной инфраструктуры автоматизированной системы и ее безопасности	Устный опрос
ПК-11 Способностью разрабатывать политику	Способен разрабатывать политику информационной безопасности	**Знания:** Основные правила разработки политики организации.	Устный опрос

информационной безопасности автоматизированной системы	автоматизированной системы	Компоненты политики безопасности **Умения:** Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю. **Навыки:** Внедрения политики безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	
ПК-22 Способностью участвовать в формировании политики информационной безопасности	Способен участвовать в формировании политики информационной безопасности организации и	**Знания:** Основные правила разработки политики безопасности организации. Компоненты политики безопасности	Устный опрос

организации и контролировать эффективность ее реализации	контролировать эффективность ее реализации	**Умения:** Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю **Навыки:** Внедрения политики безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	

Таблица 2 - Показатели и критерии оценивания компетенций на 2 этапе

Наименование компетенции	Критерии сформированности компетенции	Показатели	Процедура оценивания
1	2	3	4
ОК-5	Способен понимать социальную	**Знания:** Современные подходы	Устный опрос

Способностью понимать социальную значимость своей будущей профессии и. обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	значимость своей будущей профессии и. обладание высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдение норм профессиональной этики	к построению систем защиты информации **Умения:** Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. **Навыки:** Владеть методологическими принципами оценки защищенности объектов информатизации и обеспечения требуемого уровня защиты	
ОПК-5 Способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Способен применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	**Знания:** Знать принципы и методы разработки и применения систем обеспечения информации в научных исследованиях и в управлении технологическими, организационно-экономическими и социальными системами **Умения:** Уметь взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности в научных исследованиях и проектно-конструкторской деятельности, а также в управлении технологическими, экономическими и социальными системами	Устный опрос

		Навыки: Навыки пользования библиотеками прикладных программ для решения прикладных математических задач	
ПК-4 Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**Знания:** Основные правила разработки политики безопасности организации. Компоненты политики безопасности **Умения:** Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю **Навыки:** Навыки применения комплексного подхода к обеспечению информационной безопасности автоматизированных систем	Устный опрос
ПК-5 Способностью проводить анализ рисков информационной безопасности автоматизированной системы	Способен проводить анализ рисков информационной безопасности автоматизированной системы	**Знания:** Знать цели и задачи, решаемые разрабатываемыми процессами управления ИБ **Умения:** Оценивать информационные риски в автоматизированных системах **Навыки:** Навыками и методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных	Устный опрос

		систем, методы оценки информационных рисков	
ПК-11 Способностью разрабатывать политику информационной безопасности автоматизированной системы	Способен разрабатывать политику информационной безопасности автоматизированной системы	**Знания:** Принципы и методы противодействия несанкционированному информационному воздействию на информационные системы и системы передачи информации. **Умения:** Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. **Навыки:** Навыки применения комплексного подхода к обеспечению информационной безопасности объекта защиты	Устный опрос
ПК-22 Способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**Знания:** Принципы и методы противодействия несанкционированному информационному воздействию информационные системы **Умения:** Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. **Навыки:** Навыки применения комплексного подхода к обеспечению информационной безопасности объекта	Устный опрос

		защиты	

3. Шкалы оценивания.

Университет использует шкалы оценивания соответствующего государственным регламентам в сфере образования и позволяющую обеспечивать интеграцию в международное образовательное пространство. Шкалы оценивания и описание шкал оценивания представлены в таблицах 3 и 4.

Таблица 3 – Шкалы оценивания

Диапазон оценки, в баллах	**Экзамен**		**Зачет**
	европейская шкала (ECTS)	традиционная шкала	
[95;100]	**A** – (5+)	отлично – (5)	зачтено
[85;95)	**B** – (5)		
[70,85)	**C** – (4)	хорошо – (4)	
[60;70)	**D** – (3+)	удовлетворительно – (3)	
[50;60)	**E** – (3)		незачтено
[33,3;50)	**FX** – (2+)	неудовлетворительно – (2)	
[0;33,3)	**F** – (2)		

Таблица 4 - Описание шкал оценивания

ECTS	**Критерии оценивания**	**Традиционная шкала**
A	**Превосходно** – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.	**отлично (зачтено)**
B	**Отлично** – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному.	
C	**Хорошо** – теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено максимальным числом баллов, некоторые виды заданий выполнены с ошибками.	**хорошо (зачтено)**

D	**Удовлетворительно** – теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки.	**удовлетворительно (зачтено)**
E	**Посредственно** – теоретическое содержание курса освоено частично, некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены, либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному	**удовлетворительно (незачтено)**
FX	**Условно неудовлетворительно** – теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий.	**неудовлетворительно (незачтено)**
F	**Безусловно неудовлетворительно** – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, все выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к какому-либо значимому повышению качества выполнения учебных заданий.	

Таблица 5 – Формирование шкалы оценивания компетенций на различных этапах

Этапы формирования компетенций	Формирование оценки						
	незачтено			зачтено			
	неудовлетворительно		удовлетворительно		хорошо	отлично	
	F(2)	**FX(2+)**	**E(3)***	**D(3+)**	**C(4)**	**B(5)**	**A(5+)**
	[0;33,3)	[33,3;50)	[50;60)	[60;70)	[70;85)	[85;95)	[95;100)
Этап-1	0-16,5	16,5-25,0	25,0-30,0	30,0-35,0	35,0-42,5	42,5-47,5	47,5-50
Этап 2	0-33,3	33,3-50	50-60	60-70	70-85	85-95	95-100

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

Таблица – 6.1

ОК-5 Способностью понимать социальную значимость своей будущей профессии и. обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики **Этап 1**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Цели, задачи, принципы и основные направления обеспечения информационной безопасности государства	1. Безопасность – это: а) Специфическая совокупность внешних и внутренних условий деятельности, позволяющих субъекту контролировать процесс собственного существования и достигать намеченных целей указанной деятельности; б) Источник потенциального ущерба имуществу или инфраструктуре банка, причинение которого может воспрепятствовать достижению банка установленных целей; в) Мера допустимо опасных условий деятельности банка, неблагоприятные последствия которых реализуются в связи с ошибочными действиями или бездействием персонала банка. 2. Внутренняя безопасность включает: а) Регламентацию доступа пользователей и обслуживающего персонала к информации системы; б) Защиту от несанкционированного доступа к информации; в) Защиту от случайных внешних воздействий; 3. Криптография – это: а) Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности; б) Реквизит электронного документа, предназначенный для защиты данного документа от модификации; в) Наука о методах обеспечения конфиденциальности и аутентичности информации. 4. Какая концепция предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз: а) Стратегия адекватного ответа; б) Стратегия пассивной защиты;
Уметь: Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня защиты с учетом развития всех видов обеспечений вычислительных систем	1. Коммерческая тайна – это: а) Информация по счетам или вкладам своих клиентов и корреспондентов; б) Любая информация, обеспечивающая достижение преимуществ над конкурентами и извлечение прибыли; в) Информация об объемах и структуре предоставленных и полученных кредитов и депозитов; 2. Механизм электронной цифровой подписи реализует функции: а) Шифрование, сертификация; б) Аутентификация, шифрование; в) Сертификация, аутентификация.

Навыки: Профессиональной терминологией и методами теоретического обоснования в выборе оптимальной концепции информационной безопасности	1. Внешняя безопасность включает: а) Регламентацию доступа пользователей и обслуживающего персонала к информации системы; б) Защиту от несанкционированного доступа к информации; в) Регламентацию доступа пользователей и обслуживающего персонала к ресурсам системы. 2. По признаку целевой направленности угрозы делятся на: а) Угроза разглашения конфиденциальной информации, Угрозы со стороны конкурентов и со стороны криминальных структур; Угрозы имущественного характера и неимущественного характера.

Таблица-6.2

ОПК-5 Способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами **Этап 1**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Знать основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики.	1. По вероятности практической реализации угрозы делятся на: б) Имущественного и неимущественного характера; в) Угрозы со стороны нелояльных сотрудников и конкурентов; г) Потенциальные и реализованные угрозы. 2. Выберите правильный ответ. Какие существуют основные уровни обеспечения защиты информации? а) законодательный, б) организационно-административный, в) программно-технический (аппаратный), г) физический, д) вероятностный, е) распределительный.
Уметь: Уметь взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности в научных исследованиях и проектно-конструкторской деятельности, а также в управлении технологическими, экономическими и социальными	1. Выберите правильный ответ. Какое определение информации дано в Законе РФ "Об информации, информатизации и защите информации"? а) сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления, б) получение сведений из глобальной информационной сети, в) систематизированные данные об экономике, г) это результаты компьютерных решений определенных задач. 2. Выберите правильный ответ. Какие угрозы безопасности информации являются преднамеренными? а) взрыв в результате теракта, б) поджог, в) забастовка, г) ошибки персонала, д) неумышленное повреждение каналов связи, е) некомпетентное использование средств защиты, ж) утрата паролей, ключей, пропусков, з) хищение носителей информации,

системами	и) незаконное получение паролей.
Навыки: Навыки строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач.	1. Выберите правильный ответ. Что относится к правовым мерам защиты информации? а) законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, б) действия правоохранительных органов для защиты информационных ресурсов, в) организационно-административные меры для защиты информационных ресурсов, г) действия администраторов сети защиты информационных ресурсов. 2. Выберите правильный ответ. Какие имеются виды правовой ответственности за нарушение законов в области информационной безопасности? а) уголовная, б) административно-правовая, в) гражданско-правовая, г) дисциплинарная, д) материальная, е) условная, ж) договорная.

Таблица-6.3

ПК-4 Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты **Этап 1**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Угрозы безопасности и методы защиты информации в банковских информационных системах	1.По признаку целевой направленности угрозы делятся на: б) Угроза разглашения конфиденциальной информации, в) Угрозы со стороны конкурентов и со стороны криминальных структур; г) Угрозы имущественного характера и неимущественного характера. 2. Что относится к организационно-управленческой информации, которая входит в состав коммерческой тайны: а.Источники и объёмы финансирования и кредитования; b. Базы данных по клиентам; Базы данных о ведущих специалистов банка.
Уметь: Выявлять угрозы системе информационной безопасности разрабатывать комплекс мер по ее совершенствованию	1. Какие угрозы безопасности информации являются преднамеренными? а) взрыв в результате теракта, б) поджог, в) забастовка, г) ошибки персонала, д) неумышленное повреждение каналов связи, е) некомпетентное использование средств защиты,

	ж) утрата паролей, ключей, пропусков, з) хищение носителей информации, и) незаконное получение паролей. 2. Какие угрозы безопасности информации являются непреднамеренными? а) взрыв в результате теракта, б) поджог, в) забастовка, г) ошибки персонала, д) неумышленное повреждение каналов связи, е) некомпетентное использование средств защиты, ж) утрата паролей, ключей, пропусков
Навыки: Оценки эффективности систем защиты информации автоматизированных систем	1.Что относится к правовым мерам защиты информации? а) законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, б) действия правоохранительных органов для защиты информационных ресурсов, в) организационно-административные меры для защиты информационных ресурсов, г) действия администраторов сети защиты информационных ресурсов. 2. Какие правовые документы решают вопросы информационной безопасности? а) Уголовный кодекс РФ, б) Конституция РФ, в) Закон «Об информации, информатизации и защите

Таблица-6.4

ПК-5 Способностью проводить анализ рисков информационной безопасности автоматизированной системы **Этап 1**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Знать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ	1.Внешняя безопасность включает: а) Регламентацию доступа пользователей и обслуживающего персонала к информации системы; б) Защиту от несанкционированного доступа к информации; в) Регламентацию доступа пользователей и обслуживающего персонала к ресурсам системы. 2. По признаку целевой направленности угрозы делятся на: д) Угроза разглашения конфиденциальной информации, е) Угрозы со стороны конкурентов и со стороны криминальных структур; Угрозы имущественного характера и неимущественного характера.
Уметь: Определять информационную инфраструктуру и информационные	общие принципы организации безопасности банковских систем; -содержание и сущность концепции и политики безопасности банков; -правовые основы защиты конфиденциальной банковской информации;

ресурсы организации, подлежащие защите	-угрозы безопасности и методы защиты информации в банковских информационных системах; -порядок создания и особенности функционирования системы безопасности банка; -особенности аудита системы безопасности банка.
Навыки: Навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности	-анализировать состояние системы безопасности банка и правильно определять роль защиты информации в ее обеспечении; -разрабатывать нормативно-правовую документацию по созданию и управлению системы безопасности банка; -выявлять угрозы системе безопасности банка и разрабатывать комплекс мер по ее совершенствованию; -анализировать информацию, возникающую в процессе деятельности банка, вырабатывать рекомендации целесообразности ее защиты.

Таблица-6.5

ПК-11 Способностью разрабатывать политику информационной безопасности автоматизированной системы **Этап 1**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Основные правила разработки политики организации. Компоненты политики безопасности	1.Укажите основные свойства VPN Создает туннель, т.е. защищённый канал передачи данных Использует шифрование данных Реализуется в незащищенных или слабо защищенных сетях 2. Каковы функциональные возможности программы Retina WiFi Scanner Вычисляет WEP-ключи методом brute force Генерирует отчёты Обнаруживает IP-адреса и другую сетевую информацию Обнаруживает неавторизованные беспроводные устройства
Уметь: Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и	64- и 128-битное WEP-шифрование трафика на основе RC4 обеспечивает уровень безопасности Высокий Отметьте потенциально опасные с точки зрения утечек внутренней информации действия Размещение серверов в стороннем дата-центре Хранение носителей вне офиса Сервисный ремонт серверов или жестких дисков Перевозка компьютеров или носителей

экспортному контролю;	
Навыки: Внедрения политики безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	Перебор всех слов языка для взлома пароля это атака Brute Force Какого типа БД является реестр иерархическая

Таблица -6.6

ПК-22 Способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации **Этап 1**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Основные правила разработки политики безопасности организации. Компоненты политики безопасности	Решение DeviceLock является программно-аппаратным Способ построения одноранговых Wi-Fi сетей называется Ad-hoc
Уметь: Умения разработки политики безопасности организации, согласно	Какие решения применяются для контроля доступа к внешним устройствам Secret Disk ZLock

правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	DeviceLock Компьютер проверяет 10 млн. паролей в секудну. Сколько примерно времени ему потребуется, чтобы проверить методом словарной атаки все пароли для языка, содержащего 1 млн слов 0,1 секунды
Навыки: Внедрения политики безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	Сколько групп символов должен минимально содержать надежный пароль 3 Тонкий клиент - это Бездисковый компьютер-клиент в сетях с клиент-серверной или терминальной архитектурой, который переносит все или большую часть задач по обработке информации на сервер

Таблица-7.1

ОК-5 Способностью понимать социальную значимость своей будущей профессии и. обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

Этап 2

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности

Знать: Современные подходы к построению систем защиты информации	1. Что относится к организационно-управленческой информации, которая входит в состав коммерческой тайны: б) Источники и объёмы финансирования и кредитования; в) Базы данных по клиентам; 2. Базы данных о ведущих специалистов банка. По экономическому характеру угрозы делятся на: а) Потенциальные, реализуемые угрозы; б) Угрозы со стороны конкурентов, со стороны персонала банка; в) Угрозы имущественного и неимущественного характера.
Уметь: Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.	1. Выберите правильный ответ. Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность? а) доступность, б) целостность, в) конфиденциальность, г) управляемость, д) сложность. 2. Выберите правильный ответ. Что такое доступность информации? а) свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия, б) свойство системы, обеспечивать беспрепятственный доступ к информации любых субъектов, в) свойство системы, обеспечивать закрытый доступ к информации любых субъектов, г) свойство информации, заключающееся в легкости ее несанкционированного получения и дальнейшего распространения (несанкционированного копирования).
Навыки: Владеть методологическими принципами оценки защищенности объектов информатизации и обеспечения требуемого уровня защиты	1. Выберите правильный ответ. Что такое конфиденциальность информации? а) свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней, б) свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию), в) свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора, г) свойство информации, заключающееся в ее шифрования, д) свойство информации, заключающееся в ее принадлежности к определенному набору. 2. Выберите правильный ответ. Что относится к угрозам информационной безопасности? а) потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также

	неправомерному ее тиражированию, б) классификация информации, в) стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.), г) сбои и отказы оборудования (технических средств) АС, д) ошибки эксплуатации (пользователей, операторов и другого персонала), е) преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов), ж) последствия ошибок проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.), з) иерархическое расположение данных.

Таблица-7.2

ОПК-5 Способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами **Этап 2**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: научных исследованиях и в управлении технологическими, организационно-экономическими и социальными системами	1. Выберите правильный ответ. Что такое коммерческая тайна? а) информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, б) информация, к которой нет доступа на законном основании, в) информации, обладатель которой принимает меры к охране ее конфиденциальности, г) информация, содержащая в учредительных документах, д) информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов. 2. Выберите правильный ответ. Какие правовые документы решают вопросы информационной безопасности? а) Уголовный кодекс РФ, б) Конституция РФ, в) Закон «Об информации, информатизации и защите информации», г) Закон РФ «О государственной тайне», д) Закон РФ «О коммерческой тайне», е) Закон РФ «О лицензировании отдельных видов деятельности», ж) Закон РФ «Об образовании», з) Закон РФ «Об электронной цифровой подписи».
Уметь: Использовать полученные знания при реализации реальных проектов.	1. Задачи обеспечения безопасности БИС в локальных или глобальных вычислительных сетях: б) Обеспечение сохранности информации, как в памяти ЭВМ, так и на отдельных носителях; в) Обеспечение достоверности, идентификации и сохранности

	информации при ее передаче по каналам связи; г) Защита информации от несанкционированного доступа; 2. Главным элементом криптосистемы считаются: а) Алгоритмы шифрования; б) Методы распространения ключей к этим шифрам; Обе группы указанных элементов в равной степени.
Навыки: Навыки пользования библиотеками прикладных программ для решения прикладных математических задач	1. Промышленный шпионаж – это: б) получение обманным путем конфиденциальной информации, используемой в различных противоправных целях; в) уголовно наказуемое и иное противоправное деяние, посягающее на имущественные и приравненные к ним права и интересы банка либо на порядок его функционирования; г) присвоение кредитов по фиктивным банковским гарантиям подставными фирмами. 2. Аутентификация – это: а) Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности; б) Реквизит электронного документа, предназначенный для защиты данного документа от модификации; Наука о методах обеспечения конфиденциальности и аутентичности информации.

Таблица-7.3 ПК-4 Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты **Этап 2**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Основные правила разработки политики безопасности организации. Компоненты политики безопасности	1.Безопасность – это: г) Специфическая совокупность внешних и внутренних условий деятельности, позволяющих субъекту контролировать процесс собственного существования и достигать намеченных целей указанной деятельности; д) Источник потенциального ущерба имуществу или инфраструктуре банка, причинение которого может воспрепятствовать достижению банка установленных целей; е) Мера допустимо опасных условий деятельности банка, неблагоприятные последствия которых реализуются в связи с ошибочными действиями или бездействием персонала банка. 2.Внутренняя безопасность включает: г) Регламентацию доступа пользователей и обслуживающего персонала к информации системы; д) Защиту от несанкционированного доступа к информации; е) Защиту от случайных внешних воздействий;
Уметь: мения разработки политики безопасности организации, согласно правовыми	1.Криптография – это: а) Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности; б) Реквизит электронного документа, предназначенный для защиты данного документа от модификации;

нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	в) Наука о методах обеспечения конфиденциальности и аутентичности информации. 2.Какая концепция предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз: а) Стратегия адекватного ответа; б) Стратегия пассивной защиты; в)Упреждающего противодействия.
Навыки: Навыки применения комплексного подхода к обеспечению информационной безопасности автоматизированных систем	1.Задачи обеспечения безопасности ИС в локальных или глобальных вычислительных сетях: а) Обеспечение сохранности информации, как в памяти ЭВМ, так и на отдельных носителях; б) Защита информации от несанкционированного доступа; в) Обеспечение достоверности, идентификации и сохранности информации при ее передаче по каналам связи; 2.Коммерческая тайна – это: а) Информация по счетам или вкладам своих клиентов и корреспондентов; б) Любая информация, обеспечивающая достижение преимуществ над конкурентами и извлечение прибыли; Информация об объемах и структуре предоставленных и полученных кредитов и депозитов;

Таблица-7.4 ПК-5 Способностью проводить анализ рисков информационной безопасности автоматизированной системы **Этап 2**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Знать цели и задачи, решаемые разрабатываемыми процессами управления ИБ	1.Криптография – это: г) Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности; д) Реквизит электронного документа, предназначенный для защиты данного документа от модификации; е) Наука о методах обеспечения конфиденциальности и аутентичности информации. 2.Какая концепция предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз: в) Стратегия адекватного ответа; г) Стратегия пассивной защиты; в)Упреждающего противодействия.
Уметь: Оценивать информационные риски в автоматизированных системах	1. Какие угрозы безопасности информации являются преднамеренными? а) взрыв в результате теракта, б) поджог, в) забастовка, г) ошибки персонала, д) неумышленное повреждение каналов связи, е) некомпетентное использование средств защиты, ж) утрата паролей, ключей, пропусков,

	з) хищение носителей информации, и) незаконное получение паролей. 2. Какие угрозы безопасности информации являются непреднамеренными? а) взрыв в результате теракта, б) поджог, в) забастовка, г) ошибки персонала, д) неумышленное повреждение каналов связи, е) некомпетентное использование средств защиты, ж) утрата паролей, ключей, пропусков
Навыки: Навыками и методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем, методы оценки информационных рисков	3. Внешняя безопасность включает: а) Регламентацию доступа пользователей и обслуживающего персонала к информации системы; б) Защиту от несанкционированного доступа к информации; в) Регламентацию доступа пользователей и обслуживающего персонала к ресурсам системы. 4. По признаку целевой направленности угрозы делятся на: ж) Угроза разглашения конфиденциальной информации, з) Угрозы со стороны конкурентов и со стороны криминальных структур; Угрозы имущественного характера и неимущественного характера.

Таблица-7.5

ПК-11 Способностью разрабатывать политику информационной безопасности автоматизированной системы **Этап 2**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Принципы и методы противодействия несанкционированному информационному воздействию на информационные системы и системы передачи информации	IDS - это система обнаружения вторжений Какие режимы работы имеет программа Iris Decode Capture
Уметь: Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	Используется ли VPN для защиты беспроводных сетей да Какие дополнительные меры обеспечения безопасности могут использоваться в беспроводных сетях Технология VPN Использование IPSec для защиты трафика Защита беспроводного сегмента с помощью L2TP Выделение беспроводной сети в отдельный сегмент

Навыки: Навыки применения комплексного подхода к обеспечению информационной безопасности объекта защиты	Инсайдер - это член какой-либо группы людей, имеющий доступ к секретной, скрытой или какой-либо другой закрытой информации или знаниями, недоступной широкой публике Сколько root key содержит реестр Windows 5

Таблица -7.6

ПК-22 Способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации **Этап 2**

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Принципы и методы противодействия несанкционированному информационному воздействию информационные системы	В какой блок файла autorun.inf обычно прописываются вредоносные программы open Каково количество популярных паролей, которые остаются неизменными в течение последних 15 лет 500
Уметь: Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	Какой протокол VPN используется для создания защищенного сегмента локальной сети IpSec DLP (Data Leak Prevention) система защищает от утечек конфиденциальной информации из информационной системы вовне
Навыки: Навыки применения комплексного подхода к обеспечению информационной безопасности объекта защиты	Что позволяет выполнять программа Process Monitor Отслеживать сетевую активность процесса Отслеживать обращение процесса к реестру Отслеживать работу процесса с файлами Необходимы ли криптографические ключи для создания VPN-тоннеля Да

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Многообразие изучаемых тем, видов занятий, индивидуальных способностей студентов,

обуславливает необходимость оценивания знаний, умений, навыков с помощью системы процедур, контрольных мероприятий, различных технологий и оценочных средств.

Таблица 8 Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности на 1 этапе формирования компетенции

Виды занятий и контрольных мероприятий	Оцениваемые результаты обучения	Описание процедуры оценивания
1	2	3
Лекционное занятие (посещение лекций)	Знание теоретического материала по пройденным темам	Проверка конспектов лекций, тестирование
Выполнение практических (лабораторных) работ	Основные умения и навыки, соответствующие теме работы	Проверка отчета, устная (письменная) защита выполненной работы, тестирование
Самостоятельная работа (выполнение индивидуальных, дополнительных и творческих заданий)	Знания, умения и навыки, сформированные во время самоподготовки	Проверка полученных результатов, рефератов, контрольных работ, курсовых работ (проектов), индивидуальных домашних заданий, эссе, расчетно-графических работ, тестирование
Промежуточная аттестация	Знания, умения и навыки соответствующие изученной дисциплине	Экзамен или зачет, с учетом результатов текущего контроля, в традиционной форме или компьютерное тестирование

Таблица 9 Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности на 2 этапе формирования компетенции

Виды занятий и контрольных мероприятий	Оцениваемые результаты обучения	Описание процедуры оценивания
1	2	3
Лекционное занятие (посещение лекций)	Знание теоретического материала по пройденным темам	Проверка конспектов лекций, тестирование
Выполнение практических (лабораторных) работ	Основные умения и навыки, соответствующие теме работы	Проверка отчета, устная (письменная) защита выполненной работы, тестирование
Самостоятельная работа (выполнение индивидуальных, дополнительных и творческих заданий)	Знания, умения и навыки, сформированные во время самоподготовки	Проверка полученных результатов, рефератов, контрольных работ, курсовых работ (проектов), индивидуальных домашних заданий, эссе, расчетно-графических работ, тестирование
Промежуточная аттестация	Знания, умения и навыки соответствующие изученной дисциплине	Экзамен или зачет, с учетом результатов текущего контроля, в традиционной форме или компьютерное тестирование

В процессе изучения дисциплины предусмотрены следующие формы контроля: текущий, промежуточный контроль, контроль самостоятельной работы студентов.

Текущий контроль успеваемости обучающихся осуществляется по всем видам контактной и самостоятельной работы, предусмотренным рабочей программой дисциплины. Текущий контроль успеваемости осуществляется преподавателем, ведущим аудиторные занятия.

Текущий контроль успеваемости может проводиться в следующих формах:

- устная (устный опрос, собеседование, публичная защита, защита письменной работы, доклад по результатам самостоятельной работы и т.д.);
- письменная (письменный опрос, выполнение, расчетно-проектировочной и расчетно-графической работ и т.д.);
- тестовая (устное, письменное, компьютерное тестирование).

Результаты текущего контроля успеваемости фиксируются в журнале занятий с соблюдением требований по его ведению.

Устная форма позволяет оценить знания и кругозор студента, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки. Проводятся преподавателем с обучающимся на темы, связанные с изучаемой дисциплиной, рассчитана на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Уровень знаний, умений и навыков обучающегося при устном ответе во время промежуточной аттестации определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» по следующим критериям:

Оценка «5» (отлично)ставится, если:

–полно раскрыто содержание материала;

–материал изложен грамотно, в определенной логической последовательности;

–продемонстрировано системное и глубокое знание программного материала;

–точно используется терминология;

–показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации;

–продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков;

–ответ прозвучал самостоятельно, без наводящих вопросов;

–продемонстрирована способность творчески применять знание теории к решению профессиональных задач;

–продемонстрировано знание современной учебной и научной литературы;

–допущены одна – две неточности при освещении второстепенных вопросов, которые исправляются по замечанию.

Оценка «4» (хорошо) ставится, если:

–вопросы излагаются систематизировано и последовательно;

–продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер;

–продемонстрировано усвоение основной литературы.

–ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков:

в изложении допущены небольшие пробелы, не исказившие содержание ответа;

допущены один –два недочета при освещении основного содержания ответа,

исправленные по замечанию преподавателя;

допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя.

Оценка «3» (удовлетворительно)ставится, если:

–неполно или непоследовательно раскрыто содержание материала, но показано

общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала;

–усвоены основные категории по рассматриваемому и дополнительным вопросам;

–имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов;

–при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не может применить теорию в новой ситуации;

–продемонстрировано усвоение основной литературы

Оценка «2» (неудовлетворительно) ставится, если:

–не раскрыто основное содержание учебного материала;

–обнаружено незнание или непонимание большей или наиболее важной части учебного материала;

–допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов.

–не сформированы компетенции, умения и навыки.

Доклад–подготовленное студентом самостоятельно публичное выступление по представлению полученных результатов решения определенной учебно-практической,

учебно-исследовательской или научной проблемы.

Количество и вес критериев оценки доклада зависят от того, является ли доклад единственным объектом оценивания или он представляет собой только его часть.

Доклад как единственное средство оценивания эффективен, прежде всего, тогда, когда студент представляет результаты своей собственной учебно/научно-исследовательской деятельности, и важным является именно содержание и владение представленной информацией. В этом случае при оценке доклада может быть использована любая совокупность из следующих критериев:

–соответствие выступления теме, поставленным целям и задачам;

–проблемность / актуальность;

–новизна / оригинальность полученных результатов;

–глубина / полнота рассмотрения темы;

–доказательная база / аргументированность / убедительность / обоснованность выводов;

–логичность / структурированность / целостность выступления;

–речевая культура (стиль изложения, ясность, четкость, лаконичность, красота языка, учет аудитории, эмоциональный рисунок речи, доходчивость, пунктуальность, невербальное сопровождение, оживление речи афоризмами, примерами, цитатами и т.д.);

–используются ссылки на информационные ресурсы (сайты, литература);

–наглядность / презентабельность (если требуется);

–самостоятельность суждений / владение материалом / компетентность.

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Для повышения объективности оценки собеседование может проводиться группой преподавателей/экспертов. Критерии оценки результатов собеседования зависят от того, каковы цели поставлены перед ним и, соответственно, бывают разных видов:

–индивидуальное (проводит преподаватель)

–групповое (проводит группа экспертов);

–ориентировано на оценку знаний

–ситуационное, построенное по принципу решения ситуаций.

Критерии оценки при собеседовании:

- глубина и систематичность знаний;

- адекватность применяемых знаний ситуации;

-Рациональность используемых подходов;

- степень проявления необходимых качеств;

- Умение поддерживать и активизировать беседу;

- проявленное отношение к определенным

Письменная форма приучает к точности, лаконичности, связности изложения мысли. Письменная проверка используется во всех видах контроля и осуществляется как в аудиторной, так и во внеаудиторной работе. Письменные работы могут включать: диктанты, контрольные работы, эссе, рефераты, курсовые работы, отчеты по практикам, отчеты по научно-исследовательской работе студентов.

Контрольная работа - средство проверки умений применять полученные знания для решения задач определенного типа по теме, разделу или всей дисциплины. Контрольная работа – письменное задание, выполняемое в течение заданного времени (в условиях аудиторной работы –от 30 минут до 2 часов, от одного дня до нескольких недель в случае внеаудиторного задания). Как правило, контрольная работа предполагает наличие определенных ответов и решение задач.

Критерии оценки выполнения контрольной работы:

–соответствие предполагаемым ответам;

–правильное использование алгоритма выполнения действий (методики, технологии и т.д.);

–логика рассуждений;

–неординарность подхода к решению;

- правильность оформления работы.

Расчетно-графическая работа - средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю.

Критерии оценки:

–понимание методики и умение ее правильно применить;

–качество оформления (аккуратность, логичность, для чертежно-графических работ соответствие требованиям единой системы конструкторской документации);

–достаточность пояснений.

Реферат–продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения.

Критерии оценки (собственно текста реферата и защиты):

-информационная достаточность;

-соответствие материала теме и плану;

-стиль и язык изложения (целесообразное использование терминологии, пояснение новых понятий, лаконичность, логичность, правильность применения и оформления цитат и др.);

-наличие выраженной собственной позиции;

-адекватность и количество использованных источников (7 –10);

-владение материалом

Эссе-средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием концепций и аналитического инструментария соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме. Особенность эссе от реферата в том, что это – самостоятельное сочинение-размышление студента над научной проблемой, при использовании идей, концепций, ассоциативных образов из других областей наук и, искусства, собственного опыта, общественной практики и др. Эссе может использоваться на занятиях (тогда его время ограничено в зависимости от целей от 5 минут до 45 минут) или внеаудиторно.

Критерии оценки:

-наличие логической структуры построения текста (вступление с постановкой проблемы; основная часть, разделенная по основным идеям; заключение с выводами, полученными в результате рассуждения);

–наличие четко определенной личной позиции по теме эссе;

–адекватность аргументов при обосновании личной позиции

–стиль изложения (использование профессиональных терминов, цитат, стилистическое построение фраз, и т.д.)

–эстетическое оформление работы (аккуратность, форматирование текста, выделение и т.д.).

Курсовой проект/работа является важным средством обучения и оценивания образовательных результатов. Выполнение курсового проекта/работы требует не только знаний, но и многих умений, являющихся компонентами как профессиональных, так и общекультурных компетенций (самоорганизации, умений работать с информацией (в том числе, когнитивных умений анализировать, обобщать, синтезировать новую информацию), работать сообща, оценивать, рефлексировать).

Критерии оценки содержания и результатов курсовой работы могут различаться в зависимости от ее характера:

–реферативно-теоретические работы – на основе сравнительного анализа изученной литературы рассматриваются теоретические аспекты по теме, история вопроса, уровень разработанности проблемы в теории и практике, анализ подходов к решению проблемы с позиции различных теорий и т.д.;

–практические работы – кроме обоснований решения проблемы в теоретической части необходимо привести данные, иллюстрацию практической реализации теоретических положений на практике (проектные, методические, дидактические и иные разработки);

–опытно-экспериментальные работы – предполагается проведение эксперимента и обязательный анализ результатов, их интерпретации, рекомендации по практическому применению.

Примерные критерии оценивания курсовых работ/проектов складываются из трех составных частей:

1)оценка процесса выполнения проекта, осуществляемая по контрольным точкам, распределенным по времени выполнения проекта (четыре контрольные точки или еженедельно), проводится по критериям:

–умение самоорганизации, в том числе, систематичность работы в соответствии с планом,

–самостоятельность,

–активность интеллектуальной деятельности,

–творческий подход к выполнению поставленных задач,

–умение работать с информацией,

–умение работать в команде (в групповых проектах);

2) оценка полученного результата (представленного в пояснительной записке):

–конкретность и ясность формулировки цели и задач проекта, их соответствие теме;

–обоснованность выбора источников (полнота для раскрытия темы, наличие новейших работ

–журнальных публикаций, материалов сборников научных трудов и т.п.);

–глубина/полнота/обоснованность раскрытия проблемы и ее решений;

–соответствие содержания выводов заявленным в проекте целям и задачам;

–наличие элементов новизны теоретического или практического характера;

–практическая значимость; оформление работы (стиль изложения, логичность, грамотность, наглядность представления информации

–графики, диаграммы, схемы, рисунки, соответствие стандартам по оформлению текстовых и графических документов);

3) оценки выступления на защите проекта, процедура которой имитирует процесс профессиональной экспертизы:

–соответствие выступления заявленной теме, структурированность, логичность, доступность, минимальная достаточность;

–уровень владения исследуемой темой (владение терминологией, ориентация в материале, понимание закономерностей, взаимосвязей и т.д.);

–аргументированность, четкость, полнота ответов на вопросы;

–культура выступления (свободное выступление, чтение с листа, стиль подачи материала и т.д.).

Тестовая форма - позволяет охватить большое количество критериев оценки и допускает компьютерную обработку данных. Как правило, предлагаемые тесты оценки компетенций делятся на психологические, квалификационные (в учебном процессе эту роль частично выполняет педагогический тест) и физиологические.

Современный тест, разработанный в соответствии со всеми требованиями теории педагогических измерений, может включать задания различных типов (например, эссе или сочинения), а также задания, оценивающие различные виды деятельности учащихся (например, коммуникативные умения, практические умения).

В обычной практике применения тестов для упрощения процедуры оценивания как правило используется простая схема:

–отметка «3», если правильно выполнено 50 –70% тестовых заданий;

–«4», если правильно выполнено 70 –85 % тестовых заданий;

–«5», если правильно выполнено 85 –100 % тестовых заданий.

Параметры оценочного средства

Предел длительности контроля	45 мин.
Предлагаемое количество заданий из одного контролируемого подэлемента	30, согласно плана
Последовательность выборки вопросов из каждого раздела	Определенная по разделам, случайная внутри раздела
Критерии оценки:	Выполнено верно заданий
«5», если	(85-100)% правильных ответов
«4», если	(70-85)% правильных ответов
«3», если	(50-70)% правильных ответов

Промежуточная аттестация – это элемент образовательного процесса, призванный определить соответствие уровня и качества знаний, умений и навыков обучающихся, установленным требованиям согласно рабочей программе дисциплины. Промежуточная аттестация осуществляется по результатам текущего контроля.

Конкретный вид промежуточной аттестации по дисциплине определяется рабочим учебным планом и рабочей программой дисциплины.

Зачет, как правило, предполагает проверку усвоения учебного материала практических и семинарских занятий, выполнения лабораторных, расчетно-проектировочных и расчетно-графических работ, курсовых проектов (работ), а также проверку результатов учебной, производственной или преддипломной практик. Зачет, как правило, выставляется без опроса студентов по результатам контрольных работ, рефератов, других работ выполненных студентами в течение семестра, а также по результатам текущей успеваемости на семинарских занятиях, при условии, что итоговая оценка студента за работу в течение семестра (по результатам контроля знаний) больше или равна 60%. Оценка, выставляемая за зачет, может быть как квалитативного типа (по шкале наименований «зачтено»/ «не зачтено»), так и квантитативного (т.н. дифференцированный зачет с выставлением отметки по шкале порядка - «отлично, «хорошо» и т.д.)

Экзамен, как правило, предполагает проверку учебных достижений обучаемых по всей программе дисциплины и преследует цель оценить полученные теоретические знания, навыки самостоятельной работы, развитие творческого мышления, умения синтезировать полученные знания и их практического применения.

Экзамен в устной форме предполагает выдачу списка вопросов, выносимых на экзамен, заранее (в самом начале обучения или в конце обучения перед сессией). Экзамен включает, как правило, две части: теоретическую (вопросы) и практическую (задачи, практические задания, кейсы и т.д.). Для подготовки к ответу на вопросы и задания билета, который студент вытаскивает случайным образом, отводится время в пределах 30 минут. После ответа на теоретические вопросы билета, как правило, ему преподаватель задает дополнительные вопросы. Компетентностный подход ориентирует на то, чтобы экзамен обязательно включал деятельностный компонент в виде задачи/ситуации/кейса для решения.

В традиционной системе оценивания именно экзамен является наиболее значимым оценочным средством и решающим в итоговой отметке учебных достижений студента. В условиях балльно-рейтинговой системы балльный вес экзамена составляет 25 баллов.

По итогам экзамена, как правило, выставляется оценка по шкале порядка: «отлично»- 21-25 баллов; «хорошо»- 17,5-21 балл; «удовлетворительно»- 12,5-17,5 баллов; «неудовлетворительно»- 0-12,5 баллов.

6. Материалы для оценки знаний, умений, навыков и (или) опыта деятельности

Полный комплект оценочных средств для оценки знаний, умений и навыков находится у ведущего преподавателя.

1. Тестовые задания (предоставляются в полном объеме)
2. Типовые контрольные задания (предоставляются варианты заданий контрольных работ, расчетно-графических работ, индивидуальных домашних заданий, курсовых работ и проектов, темы эссе, докладов, рефератов)
3. Комплект билетов (предусматриваются для дисциплин формой промежуточной аттестации которых является экзамен.)