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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

Б1.В.ДВ.06.01 Технология защиты информации в различных отраслях деятельности

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.

ПК-3 - способностью проводить анализ защищенности автоматизированных систем

Знать:

Этап 1: Принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных

Этап 2: Средства обеспечения безопасности данных

Уметь:

Этап 1:Уметь реализовывать политику безопасности баз данных

Этап 2: Применять средства обеспечения безопасности данных

Владеть:

Этап 1: Навыки выявления организационных, программно- аппаратных и технических угроз безопасности база данных

Этап 2: Навыки проведения анализа защищенности автоматизированных систем

ПК-8 - способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем

Знать:

Этап 1: основные этапы проектирования подсистемы информационной безопасности

Этап 2: основные методы технико-экономического обоснования проектных решений

Уметь:

Этап 1: разрабатывать основные подсистемы безопасности информации

Этап 2: проводить технико-экономическое обоснование проектных решений

Владеть:

Этап 1: навыки разработки подсистем информационной безопасности

Этап 2: навыки технико-экономического обоснования проектных решений

ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности

Знать:

Этап 1: основные этапы проектирования подсистемы информационной безопасности

Этап 2: основные методы технико – экономического обоснования проектных решений

Уметь: проводить технико – экономическое обоснование проектных решений

Этап 1: разрабатывать основные подсистемы безопасности информации

Этап 2:

Владеть:

Этап 1: навыки разработки подсистем информационной безопасности

Этап 2: навыки технико - экономического обоснования проектных решений

ПК-11 – способностью разрабатывать политику информационно безопасности автоматизированной системы

Знать:

Этап 1:основные составляющие политики безопасности

Этап 2: принципы разработки политики безопасности

Уметь:

Этап 1: разрабатывать политик у безопасности

Этап 2: применять комплексный подход к обеспечению информационной безопасности

Владеть:

Этап 1: навыки разработки политики безопасности
Этап 2: применения комплексного подхода к обеспечению информационной безопасности

ПК-12 – способностью участвовать в проектировании и системы управления информационно безопасностью автоматизированной системы

Знать:
Этап 1: основные этапы проектирования подсистемы информационной безопасности
Этап 2: основные методы технико-экономического обоснования проектных решений
Уметь:
Этап 1: разрабатывать основные подсистемы безопасности информации
Этап 2: проводить технико-экономическое обоснование проектных решений
Владеть:
Этап 1: навыки разработки подсистем информационной безопасности
Этап 2: навыки технико-экономического обоснования проектных решений

ПК-13 -способностью участвовать в проектировании средств защиты информации автоматизированной системы

Знать:
Этап 1: знать принципы построения криптографических алгоритмов
Этап 2: знать криптографические стандарты и их использование в информационных системах
Уметь:
Этап 1: уметь выполнять настройки по обслуживанию криптосистем
Этап 2: уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием криптосистем
Владеть:
Этап 1: выполнения настроек по обслуживанию криптосистем;
Этап 2: осуществления мер противодействия нарушениям сетевой безопасности с использованием криптосистем

ПК-14 -способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

Знать:
Этап 1: основные этапы контрольных проверок технических средств защиты информации
Этап 2: основные принципы работы технических средств защиты информации
Уметь:
Этап 1: разрабатывать методик у контрольных проверок технических средств защиты информации
Этап 2: разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации
Владеть:
Этап 1: навыки применения контрольных проверок
Этап 2: навыки оценки эффективности применении аппаратно-программных комплексов

ПК-17 – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утеки информации

Знать:
Этап 1: методику анализа информационной безопасности
Этап 2: современные стандарты в области информационной безопасности
Уметь:

Этап 1: разрабатывать методик у анализа информационной безопасности
Этап 2: использовать стандарты в области информационной безопасности
Владеть:
Этап 1: разработки анализа информационной безопасности
Этап 2: использования стандартов в области информационной безопасности

ПК-19 – Способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы
Знать:
Этап 1: Общие методологические принципы построения комплексных систем обеспечения информационной безопасности;
Этап 2: комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем;
Уметь:
Этап 1: Умения ми работы с нормативно-правовыми актами
Этап 2: Первичными навыками работы с основными средства ми обеспечения информационной безопасности
Владеть:
Этап 1:Навыки участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности
Этап 2: Навыки управления процессом реализации комплекса мер по обеспечению информационной безопасности

ПК-21 -способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной без опасности автоматизированных систем
Знать:
Этап 1: основные этапы оформления рабочей документации
Этап 2: основные нормативные и методические документы
Уметь:
Этап 1: разрабатывать основные рабочие документы
Этап 2: применять нормативные документы в рабочей документации
Владеть:
Этап 1: навыки разработки рабочих документов
Этап 2: навыки применения нормативных документов

ПК-22 – способностью участвовать в формировании политик информационной безопасности организации и контролировать эффективность реализации
Знать:
Этап 1основные составляющие политики безопасности
Этап 2: принципы разработки политики безопасности
Уметь:
Этап 1: разрабатывать политику безопасности
Этап 2: применять комплексный подход к обеспечению информационной безопасности
Владеть:
Этап 1: навыки разработки политики безопасности
Этап 2:применения комплексного подхода к обеспечению информационной безопасности

ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы)для защиты информации ограниченного доступа
Знать:
Этап 1: основные принципы администрирования
Этап 2: современные инструментальные средства администрирования

Уметь:
Этап 1: основные принципы администрирования
Этап 2: современные инструментальные средства администрирования инструментальные средства администрирования подсистемы безопасности
Владеть:
Этап 1: навыки администрирования подсистемы безопасности
Этап 2: навыки применения инструментальных средств администрирования подсистемы безопасности

ПК-27 – способностью выполнять полный объем работ ,связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы
Знать:
Этап 1: основные меры по выполнения обеспечения информационной безопасности
Этап 2: основные меры поддержки обеспечения информационной безопасности
Уметь:
Этап 1: разрабатывать меры по обеспечению информационной безопасности
Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности
Владеть:
Этап 1: разработки мер по обеспечению информационной безопасности
Этап 2: разработки мер поддержки обеспечения информационной безопасности

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
ПК-3 - способностью проводить анализ защищенности автоматизированных систем	Способностью проводить анализ защищенности автоматизированных систем	**Знать:** Принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных **Уметь:** Уметь реализовывать политику безопасности баз данных **Владеть:** Навыки выявления организационных, программно- аппаратных и технических угроз безопасности база данных	Индивидуальный устный опрос, письменный опрос, тестирование

ПК-8 -способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	**Знать:** основные этапы проектирования подсистемы информационной безопасности **Уметь:** разрабатывать основные подсистемы безопасности информации **Владеть:** навыки разработки подсистем информационной безопасности	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**Знать:** основные этапы проектирования подсистемы информационной безопасности **Уметь:** разрабатывать основные подсистемы безопасности информации **Владеть:** навыки разработки подсистем информационной безопасности	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-11 – способностью разрабатывать политику информационно безопасности автоматизированной системы	Способностью разрабатывать политику информационно безопасности автоматизированной системы	**Знать:** основные составляющие политики безопасности **Уметь:** разрабатывать политик у безопасности **Владеть:** навыки разработки политики безопасности	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-12 – способностью участвовать в проектировании и системы управления информационно безопасностью автоматизированной системы	Способностью участвовать в проектировании и системы управления информационно безопасностью автоматизированной системы	**Знать:** основные этапы проектирования подсистемы информационной безопасности **Уметь:** разрабатывать основные подсистемы безопасности информации **Владеть:** навыки разработки подсистем информационной безопасности	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-13 -способностью участвовать в проектировании средств защиты информации	Способностью участвовать в проектировании средств защиты информа-	**Знать:** знать принципы построения криптографических алгоритмов **Уметь:**	Индивидуальный устный опрос, письменный опрос, тестиро-

автоматизированной системы	ции автоматизированной системы	уметь выполнять настройки по обслуживанию криптосистем **Владеть:** выполнения настроек по обслуживанию криптосистем	вание
ПК-14 -способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**Знать:** основные этапы контрольных проверок технических средств защиты информации **Уметь:** разрабатывать методик у контрольных проверок технических средств защиты информации **Владеть:** навыки применения контрольных проверок	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-17 – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утеки информации	Способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утеки информации	**Знать:** методику анализа информационной безопасности **Уметь:** разрабатывать методик у анализа информационной безопасности **Владеть:** разработки анализа информационной безопасности	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-19 – Способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	**Знать:** Общие методологические принципы построения комплексных систем обеспечения информационной безопасности; **Уметь:** Умения ми работы с нормативно-правовыми актами **Владеть:** Навыки участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-21 -способностью разрабатывать проекты документов, рег-	Способностью разрабатывать проекты документов,	**Знать:** основные этапы оформления рабочей документации	Индивидуальный устный опрос, письменный

ламентирующих работу по обеспечению информационной безопасности автоматизированных систем	регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	**Уметь:** разрабатывать основные рабочие документы **Владеть:** навыки разработки рабочих документов	опрос, тестирование
ПК-22 – способностью участвовать в формировании политик информационной безопасности организации и контролировать эффективность реализации	Способностью участвовать в формировании политик информационной безопасности организации и контролировать эффективность реализации	**Знать:** основные составляющие политики безопасности **Уметь:** разрабатывать политику безопасности **Владеть:** навыки разработки политики безопасности	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы)для защиты информации ограниченного доступа	Способностью формировать комплекс мер (правила, процедуры, методы)для защиты информации ограниченного доступа	**Знать:** основные принципы администрирования **Уметь:** основные принципы администрирования **Владеть:** навыки администрирования подсистемы безопасности	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	**Знать:** основные меры по выполнения обеспечения информационной безопасности **Уметь:** разрабатывать меры по обеспечению информационной безопасности **Владеть:** разработки мер по обеспечению информационной безопасности	Индивидуальный устный опрос, письменный опрос, тестирование

Таблица 2 - Показатели и критерии оценивания компетенций на 2 этапе

Наименование компетенции	Критерии сформированности компетенции	Показатели	Процедура оценивания
1	2	3	4
ПК-3 - способностью	Способность прово-	**Знать:**	Индивидуальный устный опрос,

проводить анализ защищенности автоматизированных систем	дить анализ защищенности автоматизированных систем	Средства обеспечения безопасности данных **Уметь:** Применять средства обеспечения безопасности данных **Владеть:** Навыки проведения анализа защищенности автоматизированных систем	письменный опрос, тестирование
ПК-8 -способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	**Знать:** основные методы технико-экономического обоснования проектных решений **Уметь:** проводить технико-экономическое обоснование проектных решений **Владеть:** навыки технико-экономического обоснования проектных решений	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**Знать:** основные методы технико – экономического обоснования проектных решений **Уметь:** проводить технико – экономическое обоснование проектных решений **Владеть:** навыки технико - экономического обоснования проектных решений	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-11 – способностью разрабатывать политику информационно безопасности автоматизированной системы	Способность разрабатывать политику информационно безопасности автоматизированной системы	**Знать:** принципы разработки политики безопасности **Уметь:** применять комплексный подход к обеспечению информационной безопасности **Владеть:** применения комплексного подхода к обеспечению информационной безопасности	Индивидуальный устный опрос, письменный опрос, тестирование

ПК-12 – способностью участвовать в проектировании и системы управления информационно безопасностью автоматизированной системы	Способность участвовать в проектировании и системы управления информационно безопасностью автоматизированной системы	**Знать:** основные методы технико-экономического обоснования проектных решений **Уметь:** проводить технико-экономическое обоснование проектных решений **Владеть:** навыки технико-экономического обоснования проектных решений	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-13 - способностью участвовать в проектировании средств защиты информации автоматизированной системы	Способность участвовать в проектировании средств защиты информации автоматизированной системы	**Знать:** знать криптографические стандарты и их использование в информационных системах **Уметь:** уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием криптосистем **Владеть:** осуществления мер противодействия нарушениям сетевой безопасности с использованием криптосистем	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**Знать:** основные принципы работы технических средств защиты информации **Уметь:** разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации **Владеть:** навыки оценки эффективности применении аппаратно-программных комплексов	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-17 – способностью проводить инструментальный мо-	Способность проводить инструментальный мониторинг за-	**Знать:** современные стандарты в области информацион-	Индивидуальный устный опрос, письменный оп-

ниторинг защищенности информации в автоматизированной системе и выявлять каналы утеки информации	щищенности информации в автоматизированной системе и выявлять каналы утеки информации	ной безопасности **Уметь:** использовать стандарты в области информационной безопасности **Владеть:** использования стандартов в области информационной безопасности	рос, тестирование
ПК-19 – Способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	**Знать:** комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем; **Уметь:** Первичными навыками работы с основными средства ми обеспечения информационной безопасности **Владеть:** Навыки управления процессом реализации комплекса мер по обеспечению информационной безопасности	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-21 - способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	**Знать:** основные нормативные и методические документы **Уметь:** применять нормативные документы в рабочей документации **Владеть:** навыки применения нормативных документов	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-22 – способностью участвовать в формировании политик информационной безопасности организации и контролировать эффективность реализации	Способность участвовать в формировании политик информационной безопасности организации и контролировать эффективность реализации	**Знать:** принципы разработки политики безопасности **Уметь:** применять комплексный подход к обеспечению информационной безопасности **Владеть:** применения комплексного подхода к обеспечению информационной	Индивидуальный устный опрос, письменный опрос, тестирование

		безопасности	
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы)для защиты информации ограниченного доступа	Способность формировать комплекс мер (правила, процедуры, методы)для защиты информации ограниченного доступа	**Знать:** современные инструментальные средства администрирования **Уметь:** современные инструментальные средства администрирования инструментальные средства администрирования подсистемы безопасности **Владеть:** навыки применения инструментальных средств администрирования подсистемы безопасности	Индивидуальный устный опрос, письменный опрос, тестирование
ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	**Знать:** основные меры поддержки обеспечения информационной безопасности **Уметь:** разрабатывать меры поддержки по обеспечению информационной безопасности **Владеть:** разработки мер поддержки обеспечения информационной безопасности	Индивидуальный устный опрос, письменный опрос, тестирование

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	**неудовлетворительно (незачтено)**

	дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий.	
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

3. 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 - ПК-3 - способностью проводить анализ защищенности автоматизированных систем. **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: Принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных	1. Содержание и структура понятия «безопасность». 2. Содержание и структура понятия «информационная безопасность». 3.Содержание и структура понятия «обеспечение информационной безопасности».
Уметь: Уметь реализовывать политику безопасности баз данных	4. Принципы защиты информации от несанкционированного доступа. 5. Информационное оружие как угроза безопасности информации. 6. Системная классификация и общий анализ угроз безопасности информации.
Навыки: Навыки выявления организационных, программно-аппаратных и технических угроз безопасности база данных	7. Источники угроз безопасности информации. 8. Основные виды технических каналов и источников утечки информации. 9. Способы предотвращения утечки информации по техническим каналам.

Таблица 7 - ПК-8 -способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем. **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 этапы проектирования подсистемы информационной безопасности	1. Доктрина информационной безопасности РФ. Основные составляющие национальных интересов РФ. 2. Дать определение понятию «информационная безопасность». Пояснить составляющие. 3. Каковы цели обеспечения информационной безопасности. Дать определение составляющим.
Уметь: разрабатывать основные подсистемы безопасности информации	4. Дать определение понятию «система защиты информации. 5. Дать определение понятию «угроза». 6. Дать определение понятию «угроза конфиденциальности».
Навыки: навыки разработки подсистем информационной безопасности	7. Дать определение понятию «угроза доступности» 8. Дать определение понятию «угроза целостности». 9. Дать определение понятию «источник угроз»

Таблица 8 - ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности. **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 этапы проектирования подсистемы информационной безопасности	1. Поясните теоретические основы ИБ АС. 2. Организационные мероприятия по работе с персоналом, получающим доступ к информации ограниченного доступа
Уметь: разрабатывать основные подсистемы безопасности информации	3. Расскажите основные подходы в управлении ИБ АС. 4. Основные процедуры приема сотрудников на работу с информацией ограниченного доступа.
Навыки: навыки разработки подсистем информационной безопасности	5. Поясните основные способы определения слабых мест в защите системы 6. Порядок оформления допуска к государственной тайне..

Таблица 9 - ПК-11 – способностью разрабатывать политику информационно 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 составляющие политики безопасности	1. Какие внешние угрозы информационной безопасности РФ в сфере внешней политики представляют наибольшую опасность? Персонал как источник угрозы безопасности информации.
Уметь: разрабатывать политик у безопасности	2. Методы добывания информации через персонал. 3. Подготовительные этапы по приему сотрудников на работу с информацией ограниченного доступа и их характеристика.
Навыки: навыки разработки политики безопасности	4. Понятие и характеристика разрешительной системы допуска к информации ограниченного доступа. Требования режима секретности по работе с секретными документами.

Таблица 10 - ПК-12 – способностью участвовать в проектировании и системы управления информационно безопасностью 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 этапы проектирования подсистемы информационной безопасности	1. Защита информации при проведении переговоров. 2. Безопасность информации в рекламно- выставочных материалах. 3. Особенности защиты информации при работе с посетителями.

Уметь: разрабатывать основные подсистемы безопасности информации	4. Основные правила организации приема посетителей. 5. Контрольно-пропускной режим на предприятии. 6. Методы и этапы отбора, подбора и найма персонала
Навыки: навыки разработки подсистем информационной безопасности	7. Нетрадиционные методы подбора персонала. 8. Взаимодействие службы безопасности с органами правопорядка. 9. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.

Таблица 11 - ПК-13 -способностью участвовать в проектировании средств защиты информации 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 принципы построения криптографических алгоритмов	1. Типовая структура служба безопасности объекта. 2. Права, обязанности и ответственность сотрудников службы безопасности. 3. Угрозы ИБ на объекте
Уметь: уметь выполнять настройки по обслуживанию криптосистем	4. Виды угроз безопасности 5. Цели создания системы обеспечения информационной безопасности. Организационная структура системы обеспечения информационной безопасности АС организации
Навыки: выполнения настроек по обслуживанию криптосистем	6. Правовые основы создания службы безопасности. 7. Основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты Технология управления информационной безопасностью

Таблица 12 - ПК-14 -способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации. **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 этапы контрольных проверок технических средств защиты информации	1. Содержание и структура понятия «безопасность». 2. Содержание и структура понятия «информационная безопасность». 3.Содержание и структура понятия «обеспечение информационной безопасности».
Уметь: разрабатывать методик у контрольных проверок технических средств защиты информации	4. Принципы защиты информации от несанкционированного доступа. 5. Информационное оружие как угроза безопасности информации. 6. Системная классификация и общий анализ угроз безопасности информации.
Навыки: навыки	7. Источники угроз безопасности информации.

применения контрольных проверок	8. Основные виды технических каналов и источников утечки информации. Способы предотвращения утечки информации по техническим каналам.

Таблица 13 - ПК-17 – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утеки информации. **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: методику анализа информационной безопасности	1. Доктрина информационной безопасности РФ. Основные составляющие национальных интересов РФ. 2. Дать определение понятию «информационная безопасность». Пояснить составляющие. Каковы цели обеспечения информационной безопасности. Дать определение составляющим.
Уметь: разрабатывать методик у анализа информационной безопасности	3. Дать определение понятию «система защиты информации. 4. Дать определение понятию «угроза». 5. Дать определение понятию «угроза конфиденциальности».
Навыки: разработки анализа информационной безопасности	6. Дать определение понятию «угроза доступности» 7. Дать определение понятию «угроза целостности». 8. Дать определение понятию «источник угроз» .

Таблица 14 - ПК-19 – Способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью 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: Общие методологические принципы построения комплексных систем обеспечения информационной безопасности;	1. Какие внешние угрозы информационной безопасности РФ в сфере внешней политики представляют наибольшую опасность? 2. Персонал как источник угрозы безопасности информации. 3. Организационные мероприятия по работе с персоналом, получающим доступ к информации ограниченного доступа.
Уметь: Умения ми работы с нормативно-правовыми актами	4. Методы добывания информации через персонал. 5. Подготовительные этапы по приему сотрудников на работу с информацией ограниченного доступа и их характеристика. 5. Основные процедуры приема сотрудников на работу с информацией ограниченного доступа.
Навыки: Навыки уча-	6. Понятие и характеристика разрешительной системы допуска

стия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности	к информации ограниченного доступа. 7. Требования режима секретности по работе с секретными документами. 8. Порядок оформления допуска к государственной тайне.

Таблица 15 - ПК-21 -способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем. **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 этапы оформления рабочей документации	1. Защита информации при проведении переговоров. 2. Безопасность информации в рекламно- выставочных материалах. 3. Особенности защиты информации при работе с посетителями.
Уметь: разрабатывать основные рабочие документы	4. Основные правила организации приема посетителей. 5. Контрольно-пропускной режим на предприятии. 6. Методы и этапы отбора, подбора и найма персонала
Навыки: навыки разработки рабочих документов	7. Нетрадиционные методы подбора персонала. 8. Взаимодействие службы безопасности с органами правопорядка. 9. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.

Таблица 16 - ПК-22 – способностью участвовать в формировании политик информационной безопасности организации и контролировать эффективность 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 составляющие политики безопасности	1. Типовая структура служба безопасности объекта. 2. Права, обязанности и ответственность сотрудников службы безопасности. 3. Угрозы ИБ на объекте
Уметь: разрабатывать политику безопасности	4. Виды угроз безопасности 5. Цели создания системы обеспечения информационной безопасности. 6. Организационная структура системы обеспечения информационной безопасности АС организации

Навыки: навыки разработки политики безопасности	7. Правовые основы создания службы безопасности. 8. Основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты 9. Технология управления информационной безопасностью

Таблица 17 - ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы)для защиты информации ограниченного доступа. **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 принципы администрирования	1. Содержание и структура понятия «безопасность». 2. Содержание и структура понятия «информационная безопасность». 3.Содержание и структура понятия «обеспечение информационной безопасности».
Уметь: основные принципы администрирования	4. Принципы защиты информации от несанкционированного доступа. 5. Информационное оружие как угроза безопасности информации. 6. Системная классификация и общий анализ угроз безопасности информации.
Навыки: навыки администрирования подсистемы безопасности	7. Источники угроз безопасности информации. 8. Основные виды технических каналов и источников утечки информации. 9. Способы предотвращения утечки информации по техническим каналам.

Таблица 18 - ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит 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 меры по выполнения обеспечения информационной безопасности	1. Доктрина информационной безопасности РФ. Основные составляющие национальных интересов РФ. 2. Дать определение понятию «информационная безопасность». Пояснить составляющие. 3. Каковы цели обеспечения информационной безопасности. Дать определение составляющим.
Уметь: разрабатывать меры по обеспечению информационной безопасности	4. Дать определение понятию «система защиты информации. 5. Дать определение понятию «угроза». 6. Дать определение понятию «угроза конфиденциальности».

Навыки: разработки мер по обеспечению информационной безопасности	7. Дать определение понятию «угроза доступности» 8. Дать определение понятию «угроза целостности». Дать определение понятию «источник угроз»

Таблица 19 - ПК-3 - способностью проводить анализ защищенности автоматизированных систем. **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: Средства обеспечения безопасности данных	1. Организационно – правовое обеспечение защиты информации. (Организационно- правовая основа, юридические аспекты). 2. Концепция комплексной системы защиты информации (Схема функций и результатов защиты информации) 3. Документ как предмет и процесс. Защита информационных технологий. Структура понятия информации (сведения и сообщения). Свойства информации в форме сведений и сообщений.
Уметь: Применять средства обеспечения безопасности данных	4. Определение информации в задачах информационной безопасности. Автономная информация. Информация воздействия. Информация взаимодействия. 5. Определение информации в задачах информационной безопасности. Автономная информация. Информация взаимодействия. 6. Информация и данные. Собственные свойства информации.
Навыки: Навыки проведения анализа защищенности автоматизированных систем	7. Информация и данные. Потребительские свойства информации. 8. Особенности и структура экономической информации. 9. Понятия компьютерного преступления.

Таблица 20 - ПК-8 -способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем. **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 методы технико-экономического обоснования проектных решений	1. Классифицировать источники угроз. 2. Дать определение понятию «уязвимость». 3. Классифицировать способы воздействия угроз.
Уметь: проводить технико-экономическое обоснование проектных	4. Виды реализации информационных угроз (перечислить, пояснить механизм реализации). 5. Виды реализации организационно-правовых угроз (перечислить, пояснить механизм реализации)

решений	6. Что наиболее подвержено воздействию угроз информационной безопасности РФ?
Навыки: навыки технико-экономического обоснования проектных решений	7. Основные меры по обеспечению информационной безопасности РФ в сфере экономики? 8. Объекты обеспечения информационной безопасности РФ во внутренней политике? 9. Угрозы информационной безопасности РФ в сфере внутренней политики.

Таблица 21 - ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности. **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 этапы проектирования подсистемы информационной безопасности	1. К какой категории угроз ИБ относится программа-шпион? 2. Понятие и основные принципы защищенного документооборота.
Уметь: разрабатывать основные подсистемы безопасности информации	3. Выберите систему и разработайте для нее политику ИБ. 4. Принципы учета и контроля документов ограниченного доступа.
Навыки: навыки разработки подсистем информационной безопасности	5. Для предложенной Вами системы укажите наиболее слабые места в ее защите, а также оцените их. 6. Защита информации при проведении совещаний.

Таблица 22 - ПК-11 – способностью разрабатывать политику информационно 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 разработки политики безопасности	1. Содержание текущей работы с персоналом, владеющим информацией ограниченного доступа. 2. Особенности увольнения сотрудников, владеющих информацией ограниченного доступа.
Уметь: применять комплексный подход к обеспечению информационной безопасности	3. Основные требования к технологической системе обработки и хранения документов ограниченного доступа. 4. Виды технологических систем обработки и хранения документов ограниченного доступа и их характеристика.
Навыки: применения комплексного подхода к обеспечению информационной безопасности	5. Проверка наличия документов ограниченного доступа. 6. Порядок уничтожения документов ограниченного доступа.

Таблица 23 - ПК-12 – способностью участвовать в проектировании и системы управления информационно безопасностью 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: основные методы технико-экономического обоснования проектных решений	1. Автотранспортные КПП. 2. Концептуальные положения организационного обеспечения информационной безопасности 3. Модель типового объекта защиты и ее характеристика.
Уметь: проводить технико-экономическое обоснование проектных решений	4. Виды и модель угроз безопасности. 5. Классификация организационных мероприятий по созданию и функционированию комплексной системы защиты. 6. Разовые организационные мероприятия и их характеристика.
Навыки: навыки технико-экономического обоснования проектных решений	7. Периодически проводимые организационные мероприятия и их характеристика. 8. Постоянно проводимые организационные мероприятия и их характеристика. 9. Цели, задачи и функции службы безопасности объекта.

Таблица 24 - ПК-13 -способностью участвовать в проектировании средств защиты информации 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 криптографические стандарты и их использование в информационных системах	1. Основы для построения и развития СУИБ 2. План развития системы информационной безопасности 3. Активы организации.
Уметь: уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием криптосистем	4. Модель нарушителя. 5. Политика информационной безопасности организации. 6. Методы расчета риска.
Навыки: осуществления мер противодействия нарушениям сетевой безопасности с использованием криптосистем	7. Подходы к анализу ИБ предприятия. 8. Определение понятия «государственная тайна». Перечень сведений, составляющих государственную тайну. 9. Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей.

Таблица 25 - ПК-14 -способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации. **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 принципы работы технических средств защиты информации	1. Организационно – правовое обеспечение защиты информации. (Организационно- правовая основа, юридические аспекты). 2. Концепция комплексной системы защиты информации (Схема функций и результатов защиты информации) 3.Документ как предмет и процесс. Защита информационных технологий. Структура понятия информации (сведения и сообщения). Свойства информации в форме сведений и сообщений.
Уметь: разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации	3. Определение информации в задачах информационной безопасности. Автономная информация. Информация воздействия. Информация взаимодействия. 4. Определение информации в задачах информационной безопасности. Автономная информация. Информация взаимодействия. 5. Информация и данные. Собственные свойства информации.
Навыки: навыки оценки эффективности применении аппаратно-программных комплексов	6. Информация и данные. Потребительские свойства информации. 7. Особенности и структура экономической информации. 8. Понятия компьютерного преступления.

Таблица 26 - ПК-17 – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утеки информации. **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 стандарты в области информационной безопасности	1. Классифицировать источники угроз. 2. Дать определение понятию «уязвимость». 3. Классифицировать способы воздействия угроз.
Уметь: использовать стандарты в области информационной безопасности	4. Виды реализации информационных угроз (перечислить, пояснить механизм реализации). 5. Виды реализации организационно-правовых угроз (перечислить, пояснить механизм реализации) 6.Что наиболее подвержено воздействию угроз информационной безопасности РФ?

Навыки: использования стандартов в области информационной безопасности	6. Основные меры по обеспечению информационной безопасности РФ в сфере экономики? 7. Объекты обеспечения информационной безопасности РФ во внутренней политике? Угрозы информационной безопасности РФ в сфере внутренней политики.

Таблица 27 - ПК-19 – Способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью 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: комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем;	1. Содержание текущей работы с персоналом, владеющим информацией ограниченного доступа. 2. Особенности увольнения сотрудников, владеющих информацией ограниченного доступа. 3. Понятие и основные принципы защищенного документооборота.
Уметь: Первичными навыками работы с основными средства ми обеспечения информационной безопасности	4. Основные требования к технологической системе обработки и хранения документов ограниченного доступа. 5. Виды технологических систем обработки и хранения документов ограниченного доступа и их характеристика. 6. Принципы учета и контроля документов ограниченного доступа.
Навыки: Навыки управления процессом реализации комплекса мер по обеспечению информационной безопасности	7. Проверка наличия документов ограниченного доступа. 8. Порядок уничтожения документов ограниченного доступа. 9. Защита информации при проведении совещаний.

Таблица 28 - ПК-21 -способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем.
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 нормативные и методические документы	1. Автотранспортные КПП. 2. Концептуальные положения организационного обеспечения информационной безопасности 3. Модель типового объекта защиты и ее характеристика.

Уметь: применять нормативные документы в рабочей документации	4. Виды и модель угроз безопасности. 5. Классификация организационных мероприятий по созданию и функционированию комплексной системы защиты. 6. Разовые организационные мероприятия и их характеристика.
Навыки: навыки применения нормативных документов	7. Периодически проводимые организационные мероприятия и их характеристика. 8. Постоянно проводимые организационные мероприятия и их характеристика. 9. Цели, задачи и функции службы безопасности объекта.

Таблица 29 - ПК-22 – способностью участвовать в формировании политик информационной безопасности организации и контролировать эффективность 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 разработки политики безопасности	1. Основы для построения и развития СУИБ 2. План развития системы информационной безопасности 3. Активы организации.
Уметь: применять комплексный подход к обеспечению информационной безопасности	4. Модель нарушителя. 5. Политика информационной безопасности организации. 6. Методы расчета риска.
Навыки: применения комплексного подхода к обеспечению информационной безопасности	7. Подходы к анализу ИБ предприятия. 8. Определение понятия «государственная тайна». Перечень сведений, составляющих государственную тайну. 9. Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей.

Таблица 30 - ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы)для защиты информации ограниченного доступа. **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 инструментальные средства администрирования	1. Организационно – правовое обеспечение защиты информации. (Организационно- правовая основа, юридические аспекты). 2. Концепция комплексной системы защиты информации (Схема функций и результатов защиты информации) 3. Документ как предмет и процесс. Защита информационных

	технологий. Структура понятия информации (сведения и сообщения). Свойства информации в форме сведений и сообщений.
Уметь: современные инструментальные средства администрирования инструментальные средства администрирования подсистемы безопасности	4. Определение информации в задачах информационной безопасности. Автономная информация. Информация воздействия. Информация взаимодействия. 5. Определение информации в задачах информационной безопасности. Автономная информация. Информация взаимодействия. 6. Информация и данные. Собственные свойства информации.
Навыки: навыки применения инструментальных средств администрирования подсистемы безопасности	7. Информация и данные. Потребительские свойства информации. 8. Особенности и структура экономической информации. 9. Понятия компьютерного преступления.

Таблица 31 - ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит 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: основные меры поддержки обеспечения информационной безопасности	1. Классифицировать источники угроз. 2. Дать определение понятию «уязвимость». 3. Классифицировать способы воздействия угроз.
Уметь: разрабатывать меры поддержки по обеспечению информационной безопасности	4. Виды реализации информационных угроз (перечислить, пояснить механизм реализации). 5. Виды реализации организационно-правовых угроз (перечислить, пояснить механизм реализации) 6. Что наиболее подвержено воздействию угроз информационной безопасности РФ?
Навыки: разработки мер поддержки обеспечения информационной безопасности	7. Основные меры по обеспечению информационной безопасности РФ в сфере экономики? 8. Объекты обеспечения информационной безопасности РФ во внутренней политике? 9. Угрозы информационной безопасности РФ в сфере внутренней политики.

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 32 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 33 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 систематизированно 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.)