Аннотация к рабочей программе дисциплины «Защищённые информационные системы»

Цель преподавания дисциплины

Цель дисциплины – изучение технологий, методов и средств создания защищенных информационных систем для успешной профессиональной деятельности.

Задачи изучения дисциплины

Задачами дисциплины являются:

1. Формирование профессиональной культуры обеспечения информационной безопасности (ИБ) в ИС.
2. Изучение принципов построения защищенных ИС.
3. Ознакомление с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных ИС.
4. Изучение подходов и методов обеспечения ИБ ИС.

Индикаторы компетенций, формируемые в результате освоения дисциплины

УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними;

ОПК-1.1 Проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности

ОПК-1.2 Разрабатывает системы обеспечения информационной безопасности объекта

ОПК-1.3 Планирует и оценивает трудоёмкость проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений

ОПК-1.4 Формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности

ОПК-1.5 Разрабатывает концептуальные стратегии решения задач моделирования и проектирования автоматизированных информационных систем и систем

ОПК-2.1 Выбирает методы решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью

ОПК-2.2 Разрабатывает тестовые планы и сценарии тестирования разработанного средства обеспечения информационной безопасности

ОПК-2.3 Проектирует подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов

ОПК 2.4 Определяет характеристики систем защиты информации

ОПК-4.1 Проводит предпроектные исследования

ОПК-4.2 Обрабатывает информацию, находящуюся в глобальной компьютерной сети

ОПК-4.3 Создаёт технические задания и технические проекты при организации ОКР

ОПК-5.1 Формализует задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструментальные средства анализа безопасности

ОПК-5.2 Представляет результаты, полученные в ходе выполнения научно-исследовательского проекта, грамотно, лаконично, в достаточном объеме на русском и иностранном языках

ОПК-5.3 Применяет в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследований

Разделы дисциплины

Понятие информационной системы и рассмотрение архитектур применяемых информационных систем. Основные аспекты построения ЗИС. Описание информационной системы и особенностей ее функционирования. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя. Определение уровня защищенности данных в информационной системе. Описание угроз безопасности информации (модель угроз безопасности информации). Методы выбора системы защиты информации. Руководящие документы ФСТЭК России.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета ФиПИ
_____ Таныгин М.О.
(подпись, инициалы, фамилия)
«30» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защищённые информационные системы
(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность,
(шифр и наименование направления подготовки)

направленность (профиль) «Защищенные информационные системы»
(наименование направленности (профиля))

форма обучения очная

ОПОП ВО реализуется по модели дуального обучения

Курск – 2023

Рабочая программа дисциплины составлена:

– в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 26.11.2020 г. № 1455;

– на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол №12 от 29.05.2023).

– с учетом заказа-требования от 28.04.2023 на результаты освоения ОПОП ВО – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», реализуемой по модели дуального обучения в ФГБОУ ВО «Юго-Западный государственный университет», от ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(приложение к общей характеристике ОПОП ВО).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для дуального обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы» на совместном заседании кафедры информационной безопасности
(наименование кафедры)
с представителями ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(протокол № 8 от 29. 05. 2023).

Зав. кафедрой _____ А.Л. Марухленко

Разработчик программы
к.т.н. _____ Е.А. Кулешова

Директор научной библиотеки _____ В.Г. Макаровская

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО дуального обучения 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол № __ от __. __. 20__), на совместном заседании кафедры информационной безопасности
(наименование кафедры)
с представителями ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(протокол № __ от __. __. 20__).

Зав. кафедрой _____

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Цель дисциплины – изучение технологий, методов и средств создания защищенных информационных систем для успешной профессиональной деятельности.

1.2 Задачи дисциплины

Задачами дисциплины являются:

1. Формирование профессиональной культуры обеспечения информационной безопасности (ИБ) в ИС.
2. Изучение принципов построения защищенных ИС.
3. Ознакомление с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных ИС.
4. Изучение подходов и методов обеспечения ИБ ИС.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компции	*наименование компетенции*		
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними;	***Знать:*** Методику анализа проблемной ситуации как системы, выявляя ее составляющие и связи между ними. ***Уметь:*** Анализировать проблемную ситуацию как систему, выявляя ее составляющие и связи между ними. ***Владеть (или Иметь опыт деятельности):*** Навыками сбора, анализа и обработки информации о проблемной ситуации как системы, выявляя ее составляющие и связи между ними.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компции	*наименование компетенции*		
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	ОПК-1.1 Проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	***Знать*** Стек технологий обеспечения информационной безопасности. ***Уметь:*** Применять известные решения, направленные на повышение защищённости систем и объектов ***Владеть (****или* ***Иметь опыт деятельности):*** Соотнесения заявленных целей и возможностей технологий обеспечения информационной безопасности известным уязвимостям и угрозам информационных ситсем
		ОПК-1.2 Разрабатывает системы обеспечения информационной безопасности объекта	***Знать*** методику разработки технических систем. ***Уметь:*** выполнять декомпозицию создавамых систем на структурные и функциональные блоки ***Владеть (****или* ***Иметь опыт деятельности):*** выработки технических решений, направленных на обеспечение безопасности информационных систем
		ОПК-1.3 Планирует и оценивает трудоёмкость проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений	***Знать*** методы оценки затрат ресурсов на создание и внедрение технических систем. ***Уметь:*** формировать ресурсные требования по отдельным этапам реализации проекта создания защищённой информационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** выбора средств и технологий обеспечения информационной безопасности в условиях ограниченности ресурсов
		ОПК-1.4 Формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на	***Знать*** методику формирования модели угроз для информационной системы. ***Уметь:*** выделять и ранжировать угрозы информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** навыками формирования списка угроз, актуальных для конкретной информационной системы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компции	*наименование компетенции*		
		проектируемую систему обеспечения информационной безопасности	
		ОПК-1.5 Разрабатывает концептуальные стратегии решения задач моделирования и проектирования автоматизированных информационных систем и систем	***Знать*** возможности и инструментарий моделирования информационных систем. ***Уметь:*** делать качественные и количественных оценки различных характеристик информационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** навыками выбора принципов проектирования защищённых информационных систем на основе результатов и положений научных исследований
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	ОПК-2.1 Выбирает методы решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	***Знать*** методы, принципы правила и регламенты создания технически проектов защищенной информационной системы. ***Уметь:*** выполнять отдельные этапы и комплекс мероприятий по созданиютехнически проектов защищенной информационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками создания технически проектов защищенной информационной системы
		ОПК-2.2 Разрабатывает тестовые планы и сценарии тестирования разработанного средства обеспечения информационной безопасности	***Знать*** методику, порядок и правила проведения тестовых и экспериментальных исследований ***Уметь:*** формировать планы и сценарии оценки проведения испытаний информационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками проведения тестовых испытаний информационной системы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		ОПК-2.3 Проектирует подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов	***Знать*** нормативную базу регуляторов в области информационной безопасности. ***Уметь:*** использовать нормативное и информационное обеспечение регуляторов для формирования проектных решений ***Владеть (****или* ***Иметь опыт деятельности):*** ** навыками использования нормативно-правовых актов при проектировании защищённых информационных систем
		ОПК 2.4 Определяет характеристики систем защиты информации	***Знать*** перечень характеристик информационных систем. ***Уметь:*** формулировать протоколы определения качественных и количественных характеристик информационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** определения качественных и количественных характеристик информационных систем
ОПК-4	Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;	ОПК-4.1 Проводит предпроектные исследования	***Знать*** основные методы исследования характеристик информационных систем. ***Уметь:*** определять методы и средства для проведения предпроектных исследований и теоретически достигаемых характеристик информационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** проведения предпроектных исследований характеристик информационных систем
		ОПК-4.2 Обрабатывает информацию, находящуюся в глобальной компьютерной сети	***Знать*** основные источники патентной информации, классификацию патентных документов, патентные и справочные системы ***Уметь:*** проводить подбор источников патентной информации по заданной тематике ***Владеть (****или* ***Иметь опыт деятель-***

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компции	*наименование компетенции*		
			ности): навыками обработки информации, находящейся в глобальной компьютерной сети
		ОПК-4.3 Создаёт технические задания и технические проекты при организации ОКР	***Знать*** правила и принципы создания технических заданий на проведение работ по разработке защищённых информационных систем. ***Уметь:*** структурировать по этапам работы по разработке защищённых информационных систем и формулировать измеряемые критерии выполнения отдельных этапов ***Владеть (****или* ***Иметь опыт деятельности):*** создания технических заданий на проведение работ по разработке защищённых информационных систем.
ОПК-5	Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	ОПК-5.1 Формализует задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструментальные средства анализа безопасности	***Знать*** основные методы научного исследования характеристик информационных систем. ***Уметь:*** разрабатывать методики исследований характеристик информационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** проводить исследований характеристик информационных систем
		ОПК-5.2 Представляет результаты, полученные в ходе выполнения научно-исследовательского проекта, грамотно, лаконично, в достаточном объеме на русском и иностранном языках	***Знать*** правила оформления научной и технической документации. ***Уметь:*** описывать документально проведение работ по созданию защищённых информационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** формулирования результатов проектных и предпроектных исследований

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компции	*наименование компетенции*		
		ОПК-5.3 Применяет в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследований	***Знать*** методы экспериментального исследования защищенности объектов ***Уметь:*** Проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента ***Владеть (****или* ***Иметь опыт деятельности):*** апробация и внедрение разработанных эффективных технологий

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Защищённые информационные системы» входит в обязательную часть блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищённые информационные системы», реализуемой по модели дуального обучения.

Дисциплина изучается на 1 курсе в 1 семестре.

Дисциплина имеет практико-ориентированный характер и изучается до прохождения обучающимися производственной практики (исследовательской работы), завершающей данный семестр.

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 6 зачетных единицы (з.е.), 216 академических часов.

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	216

Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	126
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	54, из них практическая подготовка обучающихся – 4.
Самостоятельная работа обучающихся (всего)	52.85
Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен
экзамен (включая консультацию перед экзаменом)	1,15

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Понятие информационной системы и рассмотрение архитектур применяемых информационных систем	Понятие информационной системы, основные компоненты информационной системы. Виды информационных систем. Особенности различных архитектур информационных систем. Уровни организации архитектур информационных систем. Особенности распределённых информационных систем
2.	Основные аспекты построения ЗИС	Регулирование ответственности нарушений информационной безопасности. Программа информационной безопасности. Контроль деятельности в области безопасности. Модели представления информационной защиты. Формирование требований к системе информационной безопасности. Этапы обеспечения информационной безопасности.
3.	Описание информационной системы и особенностей ее функционирования	Структура и состав информационной системы. Описание физических, функциональных, технологических и логических взаимосвязей
4.	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя	Категория лиц, рассматриваемых и не рассматриваемых в качестве нарушителей. Обобщенные возможности нарушителя. Уточненные возможности нарушителя. Актуальность использования (применения) возможностей нарушителя для построения и реализации атак. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности данных

5.	Определение уровня защищенности данных в информационной системе	Определение типа угроз безопасности информации. Определение категории обрабатываемых данных. Определение количества субъектов данных. Определение уровня защищенности данных. Определение класса информационной системы. Оценка степени возможного ущерба. Определение класса защищенности информационной системы.
6.	Описание угроз безопасности информации (модель угроз безопасности информации)	Определение перечня угроз безопасности информации, возможных с учетом потенциала нарушителя. Определение перечня угроз безопасности информации, возможных с учетом применяемых технологий. Определение исходной защищенности информационной системы. Определение частоты (вероятности) реализации угроз. Определение объема негативных последствий. Способы реализации угроз безопасности информации. Возможные уязвимости информационной системы.
7.	Методы выбора системы защиты информации	Классификация методов выбора систем защиты информации. Метод анализа иерархий. Метод парных сравнений альтернатив. Многокритериальный выбор в иерархических структурах с множеством различных альтернатив под критериями. Методы принятия решений, основанные на исследовании операций. Сопоставление угроз и методов и средств их устранения. Игровые стратегии выбора системы защиты информации
8.	Руководящие документы ФСТЭК России	Требования к защищенности автоматизированных систем. Классы защищённости информационных систем. Аспекты защищённых ИС, фигурирующие в требованиях ФСТЭК. Классификация защищённых информационных систем

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Понятие информационной системы и рассмотрение архитектур применяемых информационных систем	4		1	У 1-5 МУ 1-3	УО, ЗПР, КЗ 1-2	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5
2	Основные аспекты построения ЗИС	4		2	У 1-5 МУ 1-3	УО, ЗПР 2-3	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5
3	Описание информационной системы и особенностей ее функционирования	4		3	У 1-5 МУ 1-3	УО, ЗПР 3-4	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5

4	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя	4	1	4	У 1-5 МУ 1-3	УО, ЗЛР, ЗПР 5-6	ОПК-1, ОПК-2, ОПК-4, ОПК-5
5	Определение уровня защищенности данных в информационной системе	4		5	У 1-5 МУ 1-3	УО, ЗПР, КЗ 7-8	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5
6	Описание угроз безопасности информации (модель угроз безопасности информации)	4	2	6	У 1-5 МУ 1-3	УО, ЗЛР, ЗПР 9-10	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5
7	Методы выбора системы защиты информации	6		7	У 1-5 МУ 1-3	УО, ЗПР, КЗ 11-12	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5
8	Руководящие документы ФСТЭК России	6	3	8	У 1-5 МУ 1-3	УО, ЗЛР, ЗПР, ПЗ 13-14	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5

УО – устный опрос, ЗЛР – защита лабораторной работы, ЗПР – защита практической работы, ПЗ – решение производственных задач; КЗ – решение кейса

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	Создание модели вероятного нарушителя	10
2	Составление модели угроз безопасности информационной системы	10
	Обзор руководящих документов Федеральной службы технического и экспортного контроля (ФСТЭК России)	16
Итого		36

4.2.2 Практические занятия

Таблица 4.2.2 – Практические занятия

№	Наименование практического занятия	Объем, час.
1.	Определение перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных	6
2.	Определение уровня исходной защищённости	6

3.	Определение частоты (вероятности) реализации рассматриваемой угрозы	6
4.	Определение коэффициента реализуемости угрозы и возможности реализации	6
5.	Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных	8
6.	Определение типа актуальной угрозы	6
7.	Определение уровня защищенности	8
8.	Определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах	8, из них практическая подготовка обучающихся – 4
Итого		54, из них практическая подготовка обучающихся – 4

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Понятие информационной системы и рассмотрение архитектур применяемых информационных систем	1-2 недели	6
2.	Основные аспекты построения ЗИС	2-3 недели	6
3.	Описание информационной системы и особенностей ее функционирования	4-5 недели	6
4.	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя	5-6 недели	6
5.	Определение уровня защищенности данных в информационной системе	7-8 недели	6
6.	Описание угроз безопасности информации (модель угроз безопасности информации)	8-9 недели	6
7.	Методы выбора системы защиты информации	10-11 недели	6
8.	Руководящие документы ФСТЭК России	11-14 недели	10,85
Итого			52,85

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельном изучении отдельных тем и вопросов дисциплины студенты могут пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры информационной без-

опасности в рабочее время, установленное Правилами внутреннего распорядка работников университета.

Учебно-методическое обеспечение самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с учебным планом и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– методических указаний к выполнению лабораторных и практических работ и т.д.

типографией университета:

– посредством оказания помощи авторам в подготовке и издании научной, учебной и методической литературы;

– посредством удовлетворения потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии. Практическая подготовка обучающихся

Реализация программы магистратуры по модели дуального обучения и компетентностного подхода предусматривают широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных и общепрофессиональных компетенций обучающихся.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	2	3	4
1	Описание особенностей информационной системы, влияющих на её защищённость	Кейс-технология	3
2	Определение актуальных угроз безопас-	Кейс-технология	3

	ности персональных данных при их обработке в информационных системах персональных данных		
3	Определение уровня защищенности	Кейс-технология	4
Итого:			10

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю) программы магистратуры.

Практическая подготовка обучающихся при реализации дисциплины организуется в модельных условиях.

Практическая подготовка обучающихся проводится в соответствии с положением П 02.181

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Защищённые информационные системы Современная философия и методология науки	Моделирование технических объектов и систем управления	
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Защищённые информационные системы	Производственная практика (исследовательская работа)	
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Защищённые информационные системы	Производственная практика (исследовательская работа)	
ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;	Защищённые информационные системы	Производственная практика (исследовательская работа)	
ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	Защищённые информационные системы Профессиональный иностранный язык	Производственная практика (исследовательская работа)	

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(наименование этапа по таблице 6.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за практикой)*	Критерии и шкала оценивания компетенций			
		Недостаточный уровень («неудовл.»)	Пороговый уровень («удовл.»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5	6
УК-1/ начальный	УК-1.1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для УК-1. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для УК-1. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для УК-1. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для УК-1. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для УК-1.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для УК-1.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для УК-1.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для УК-1.

		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-1, доведены до автоматизма.
ОПК-1/ начальный	ОПК-1.1 Проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности ОПК-1.2 Разрабатывает системы обеспечения информационной безопасности объекта ОПК-1.3 Планирует и оценивает трудоёмкость проекта, вклю-	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ОПК-1. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ОПК-1. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ОПК-1. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ОПК-1. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ОПК-1.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ОПК-1.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ОПК-1.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ОПК-1.

	чая техническое, кадровое и финансовое обеспечение, принятие совместных решений ОПК-1.4 Формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности ОПК-1.5 Формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании тре-	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-1, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-1, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-1, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-1, доведены до автоматизма.

	бований технического задания на проектируемую систему обеспечения информационной безопасности				
ОПК-2/ начальный	ОПК-2.1 Выбирает методы решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью ОПК-2.2 Разрабатывает тестовые планы и сценарии тестирования разработанного средства обеспечения информационной	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ОПК-2. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ОПК-2. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ОПК-2. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ОПК-2. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ОПК-2.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ОПК-2.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ОПК-2.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ОПК-2.

	безопасности ОПК-2.3 Проектирует подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов ОПК-2.4 Определяет характеристики систем защиты информации	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-2, не развиты.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-2, развиты на элементарном уровне.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-2, хорошо развиты.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-2, доведены до автоматизма.
ОПК-3/ начальный	ОПК-3.1 Проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ОПК-3. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ОПК-3. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ОПК-3. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ОПК-3. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.

	ОПК-3.2 Рассчитывает риски информационной безопасности ОПК-3.3 Выбирает инструментарий в области проектирования и управления информационной безопасности ОПК-3.4 Разрабатывает организационно-распорядительную документацию по обеспечению информационной безопасности ОПК-3.5 Разрабатывает модели угроз и нарушителей информационной безопасности информационных систем	**Уметь:** демонстрирует менее 60% умений, установленных в таблице 1.3 для ОПК-3.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ОПК-3.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ОПК-3.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ОПК-3.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-3, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-3, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-3, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-3, доведены до автоматизма.
ОПК-4/ начальный	ОПК-4.1 Проводит предпроектные исследования	**Знать:** демонстрирует менее 60% знаний, указанных в таб-	**Знать:** демонстрирует 60-74% знаний, указанных в	**Знать:** демонстрирует 75-89% знаний, указанных в таб-	**Знать:** демонстрирует 90-100% знаний, указанных в таблице

	ОПК-4.2 Обрабатывает информацию, находящуюся в глобальной компьютерной сети ОПК-4.3 Создаёт технические задания и технические проекты при организации ОКР	лице 1.3 для ОПК-4. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	таблице 1.3 для ОПК-4. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	лице 1.3 для ОПК-4. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	1.3 для ОПК-4. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ОПК-4.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ОПК-4.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ОПК-4.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ОПК-4.
		Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ОПК-4, не развиты.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-4, развиты на элементарном уровне.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-4, хорошо развиты.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-4, доведены до автоматизма.
ОПК-5/ начальный	ОПК-5.1 Формализует задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструмен-	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ОПК-5. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может ис-	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ОПК-5. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ОПК-5. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ОПК-5. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно опе-

	тальные средства анализа безопасности ОПК-5.2 Представляет результаты, полученные в ходе выполнения научно-исследовательского проекта, грамотно, лаконично, в достаточном объеме на русском и иностранном языках ОПК-5.3 Применяет в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследований	править самостоятельно.			рирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ОПК-5.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ОПК-5.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ОПК-5.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ОПК-5.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-5, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-5, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-5, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-5, доведены до автоматизма.

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

Таблица 7.3 - Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1.	Понятие информационной системы и рассмотрение архитектур применяемых информационных систем	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, практическая работа	ВУО КВЗПР Кейс	1-10 1-10 1	Согласно табл. 7.2
2.	Основные аспекты построения ЗИС	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, лабораторная работа	ВУО КВЗПР	1-10 1-10	Согласно табл. 7.2
3.	Описание информационной системы и особенностей ее функционирования	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, лабораторная работа	ВУО КВЗПР	1-10 1-10	Согласно табл. 7.2
4.	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя	ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, лабораторная работа	ВУО КВЗПР КВЗЛР	1-10 1-10 1-10	Согласно табл. 7.2
5.	Определение уровня защищенности данных в информационной системе	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, практическая работа	ВУО КВЗПР Кейс	1-10 1-10 2	Согласно табл. 7.2
6.	Описание угроз безопасности информации (модель угроз безопасности информации)	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС,	ВУО КВЗПР КВЗЛР	1-10 1-10 1-10	Согласно табл. 7.2
7.	Методы выбора системы защиты информации	УК-1, ОПК-1, ОПК-2, ОПК-4,	Лекция, СРС, лабораторная работа	ВУО КВЗПР Кейс	1-10 1-10 3	Согласно табл. 7.2

1	2	3	4	5	6	7
		ОПК-5				
8.	Руководящие документы ФСТЭК России	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, практическая работа	ВУО КВЗПР КВЗЛР Производственная задача	1-10 1-10 1-10 1-10	Согласно табл. 7.2

ВУО- вопросы для устного опроса
КВЗПР- контрольные вопросы для защиты практической работы
КВЗЛР- контрольные вопросы для защиты лабораторной работы

7.3.1 Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по теме 1 «Понятие информационной системы и рассмотрение архитектур применяемых информационных систем»

1. Что такое информационная система?
2. Какие основные компоненты входят в состав информационной системы?
3. Какие функции выполняют информационные системы?
4. Какие бывают типы информационных систем?
5. Что такое архитектура информационной системы?

Контрольные вопросы для защиты лабораторной работы 3 «Обзор руководящих документов Федеральной службы технического и экспортного контроля (ФСТЭК России)»

1. Какая организация разрабатывает руководящие документы в области технического и экспортного контроля в России?
2. Какие основные задачи выполняет Федеральная служба технического и экспортного контроля (ФСТЭК России)?
3. Что такое лицензирование при экспорте технических средств и информационных материалов?
4. Какие руководящие документы ФСТЭК России относятся к требованиям информационной безопасности?
5. Упомяните некоторые из руководящих документов ФСТЭК России, относящихся к классификации информации.

Контрольные вопросы для защиты практической работы 1 «Определение перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных»

1. Перечислите Источники угроз НСД в ИСПДн

2. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на два вида. Назовите, какие.

3. К каким видам нарушения безопасности информации может привести реализация угроз НСД?

Производственная задача

Компания разрабатывает новую защищенную информационную систему для хранения конфиденциальных данных клиентов. Опишите процесс установки и конфигурирования системы, чтобы обеспечить максимальную безопасность данных.

Кейс

Компания XYZ, занимающаяся производством и продажей товаров, решила перевести все свои бизнес-процессы на цифровую платформу. Для этого была разработана информационная система, которая должна обеспечивать хранение и обработку конфиденциальных данных, таких как данные клиентов, бухгалтерская отчётность и т.д.Однако, наш эксперт в области информационной безопасности обнаружил уязвимости в системе, которые могут привести к утечке конфиденциальных данных. Для того, чтобы избежать потенциальных проблем, было решено провести аудит системы и разработать план защиты информационной системы.

Ваша задача как специалиста по защищённым информационным системам - помочь компании XYZ разработать и реализовать план защиты информационной системы.

Ваше решение должно включать в себя:

1) Анализ уязвимостей информационной системы.

2) Разработку плана защиты информационной системы, который будет включать в себя:

3) Меры по обеспечению физической безопасности серверов и сетевых устройств.

4) Меры по защите от внешних и внутренних угроз.

5) Меры по обеспечению конфиденциальности и целостности данных.

6) План действий в случае нарушения безопасности информационной системы.

7) Рекомендации по обучению персонала по правилам безопасности информационной системы.

7.3.2 Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. На промежуточной аттестации по дисциплине применяется механизм квалификационного экзамена. Экзамен имеет структуру квалификационного экзамена и состоит из 2 частей:

– теоретической (компьютерное тестирование);

– практической (решение компетентностно-ориентированной задачи).

На теоретической части экзамена (тестировании) проверяются знания и частично – умения и навыки обучающихся. Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

– закрытой (с выбором одного или нескольких правильных ответов),

– открытой (необходимо вписать правильный ответ),

– на установление правильной последовательности,

– на установление соответствия.

На практической части экзамена проверяются результаты практической подготовки: *компетенции, включая умения, навыки (или опыт деятельности)*). Результаты практической подготовки *(компетенции, включая умения, навыки (или опыт деятельности))* проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных, кейс-задач или кейсов) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

а) Примеры типовых заданий для теоретической части экзамена (тестирования)

Задание в открытой форме:

Механизм одобрения для защищенных систем основан на…

Задание на установление правильной последовательности,

Установить последовательность этапов внедрения системы безопасности

1. Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта

2. Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению

3. Установка и настройка средств защиты информации

4. Испытания и опытная эксплуатации системы защиты информации

Задание на установление соответствия:

Для информационной ситсемы в составе нескольких защищаемых помещений с числом субъектов ПДн более 100 установите соответствие:

a. Угроза скрытной регистрации вредоносной программой учетных записей администраторов внешний нарушитель с потенциалом не ниже усиленного базового.

b. Угроза хищения аутентификационной информации из временных файлов cookie внешний нарушитель с потенциалом не ниже усиленного базового;

c. Угроза изменения системных и глобальных переменных внутренний нарушитель с потенциалом не ниже усиленного базового;

1 Опасность угрозы низкая

2 Опасность угрозы средняя

3 Опасность угрозы высокая

4 Опасность угрозы приемлемая

б) Примеры типовых заданий для практической части экзамена

Компетентностно-ориентированная задача:

Компания решила перейти на облачные технологии и использовать облачную защищенную информационную систему для хранения конфиденциальных данных о клиентах. Какие меры безопасности необходимо предпринять для защиты информации от несанкционированного доступа, взлома и утечки?

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– положение П 02.207 «Проектирование и реализация основных профессиональных программ высшего образования – программ магистратуры по модели дуального обучения»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Лабораторная работа № 1-3	3	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	6	Выполнил, правильно и полно ответил на все вопросы
Практическая работа № 1-8	8	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	16	Выполнил, правильно и полно ответил на все вопросы

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Кейс	3	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	6	Выполнил, правильно и полно ответил на все вопросы
Производственная задача	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Устный опрос по темам 1-8	8	Не ответил или неполно ответил на какой-либо вопрос	16	Правильно и полно ответил на все вопросы
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

Для проведения промежуточной аттестации обучающихся (теоретической части и практической части) используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов для тестирования и одна компетентностно-ориентированная задача).

Каждый верный ответ оценивается следующим образом:

– задание в закрытой форме –2 балла,
– задание в открытой форме – 2 балла,
– задание на установление правильной последовательности – 2 балла,
– задание на установление соответствия – 2 балла,
– решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов по промежуточной аттестации – 36.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная литература

1. Маглинец, Ю. А. Анализ требований к автоматизированным информационным системам : учебное пособие / Ю. А. Маглинец. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 191 с. — ISBN 978-5-4497-0301-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89417.html (дата обращения: 04.10.2023). — Режим доступа: для авторизир. Пользователей

2. Мартынов, А. П. Информационная безопасность и защита информации : учебное пособие / А. П. Мартынов, И. А. Мартынова, А. А. Русаков. — Москва : Ай Пи Ар Медиа, 2023. — 122 с. — ISBN 978-5-4497-2247-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/131797.html (дата обращения: 04.10.2023). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/131797

8.2 Дополнительная литература

3. Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский. — Новосибирск : Новосибирский государственный технический университет, 2018. — 80 с. — ISBN 978-5-7782-3517-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/91285.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

4. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

5. Долженко, А. И. Управление информационными системами : учебное пособие / А. И. Долженко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 180 с. — ISBN 978-5-4497-0911-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102074.html (дата обращения: 03.10.2023). — Режим доступа: для авторизир. Пользователей

8.3 Перечень методических указаний

1) Защищенные информационные системы: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 11 с.: Библиогр.: с. 11.

2) Защищенные информационные системы: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 55 с.: Библиогр.: с. 54.

3) Защищенные информационные системы: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 17 с.: Библиогр.: с. 17.

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3. Электронно-библиотечная система «Лань» - http://e.lanbook.com/
4. Электронно-библиотечная система IQLib – http://www.iqlib.ru
5. Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru/

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции и лабораторные и практические занятия.

На лекциях излагаются и разъясняются основные понятия и положения каждой новой темы; важные положения аргументируются и иллюстрируются примерами из практики; объясняется практическая значимость изучаемой темы; делаются выводы; даются рекомендации для самостоятельной работы по данной теме. На лекциях необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных вопросов. В ходе лекции студент должен конспектировать учебный материал. Конспектирование лекций – сложный вид работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это лично студентом в режиме реального времени в течение лекции. Не следует стремиться записать лекцию дословно. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем кратко записать ее. Желательно заранее оставлять в тетради пробелы, куда позднее, при самостоятельной работе с конспектом, можно внести дополнительные записи. Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, который преподаватель дает в начале лекционного занятия. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале.

Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологией. Работу с конспектом лекции целесообразно проводить непосредственно после ее прослушивания, что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях. Работа с конспектом лекции предполагает перечитывание конспекта, внесение в него, по необходимости, уточнений, дополнений, разъяснений и изменений. Некоторые вопросы выносятся за рамки лекций. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы, указанной в п.8.2.

Изучение наиболее важных тем или разделов дисциплины продолжается на лабораторных и практических занятиях, которые обеспечивают контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному и практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. При работе с источниками и литературой необходимо:

– сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;

– обобщать полученную информацию, оценивать прочитанное;

– фиксировать основное содержание прочитанного текста; формулировать устно и письменно основную идею текста; составлять план, формулировать тезисы.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю. Обязательным элементом самостоятельной работы по дисциплине является самоконтроль. Одной из важных задач обучения студентов способам и приемам самообразования является формирование у них умения самостоятельно контролировать и адекватно оценивать результаты своей учебной деятельности и на этой основе управлять процессом овладения знаниями. Овладение умениями самоконтроля приучает студентов к планированию учебного труда, способ-

ствует углублению их внимания, памяти и выступает как важный фактор развития познавательных способностей. Самоконтроль включает:

– оперативный анализ глубины и прочности собственных знаний и умений;

– критическую оценку результатов своей познавательной деятельности.

Самоконтроль учит ценить свое время, позволяет вовремя заметить и исправить свои ошибки. Формы самоконтроля могут быть следующими:

– устный пересказ текста лекции и сравнение его с содержанием конспекта лекции;

– составление плана, тезисов, формулировок ключевых положений текста по памяти;

– пересказ с опорой на иллюстрации, чертежи, схемы, таблицы, опорные положения.

Самоконтроль учебной деятельности позволяет студенту оценивать эффективность и рациональность применяемых методов и форм умственного труда, находить допускаемые недочеты и на этой основе проводить необходимую коррекцию своей познавательной деятельности.

При подготовке к промежуточной аттестации по дисциплине необходимо повторить основные теоретические положения каждой изученной темы и основные термины, самостоятельно решить несколько типовых компетентностно-ориентированных задач.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Информационные технологии:

1. Средства для просмотра презентаций;
2. Средства для проведения онлайн-конференций.
3. Электронно-образовательная среда ЮЗГУ

Программное обеспечение:

1. OpenOffice: режим доступа: свободный.
2. Яндекс.Телемост: режим доступа: свободный.

Информационные справочные системы:

1. Научно-информационный портал ВИНИТИ РАН. Режим доступа: свободный.
2. База данных "Патенты России". Режим доступа: свободный.
3. Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: по подписке.

4. Электронная библиотека диссертаций и авторефератов РГБ. Режим доступа: свободный.

5. Электронный каталог Научной библиотеки ЮЗГУ. Режим доступа: свободный.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудиторные занятия по дисциплине проводятся в учебной аудитории для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенных стандартной учебной мебелью (столы и стулья для обучающихся; стол и стул для преподавателя; доска).

Для организации образовательного процесса применяются технические средства обучения: Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24.

Для осуществления практической подготовки обучающихся при реализации дисциплины используются оборудование и технические средства обучения кафедры информационной безопасности:

1. Класс ПЭВМ - Asus-P7P55LX-/DDR34096Mb/Coree i3-540/SATA-11 500 Gb Hitachi/PCI-E 512Mb, Монитор TFT Wide 23.

2. Мультимедиацентр: ноутбук ASUS X50VL PMD - T2330/14"/1024Mb/ 160Gb/ сумка/проектор inFocus IN24+ .

3. Экран мобильный Draper Diplomat 60x60.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			