Аннотация к рабочей программе дисциплины «Защищённые информационные системы»

Цель преподавания дисциплины

Дисциплина "Защищённые информационные системы" изучается с целью изучения технологий, методов и средств создания защищенных информационных систем.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

– сформировать профессиональную культуру обеспечения информационной безопасности (ИБ) в ИС;

– понимать принципы построения защищенных ИС;

– познакомиться с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных ИС;

– изучить подходы и методы обеспечения ИБ ИС

Индикаторы клмпетенций, 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-4.2 Составляет пошаговый план научной деятельности, проводит предпроектные исследования

ОПК-4.4 Создаёт технические задания и технические проекты при организации НИОКР

ОПК-5.3 Формализует задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструментальные средства анализа безопасности

ОПК-5.4 Представляет результаты, полученные в ходе выполнения научно-исследовательского проекта грамотно, лаконично, в достаточном объеме на русском и иностранном языках

ОПК-5.5 Применяет в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследований

Разделы дисциплины

Понятие информационной системы и рассмотрение архитектур применяемых информационных систем. Основные аспекты построения системы информационной безопасности. Мероприятия по защите информации. Требования к архитектуре ИС для обеспечения безопасности ее функционирования. Оценочные стандарты и технические спецификации. Критерии оценки безопасности информационных технологий. Руководящие документы ФСТЭК России. 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.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

М.О. Таныгин
(подпись, инициалы, фамилия)
«31» 09 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защищённые информационные системы
(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность
шифр и наименование направление подготовки (специальности)

Защищённые информационные системы
наименование направленности (профиля, специализации)

форма обучения очная
очная, очно-заочная, заочная

Курск – 2021

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета (протокол № 10 «26» 02 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы» на заседании кафедры информационной безопасности №1 «30» 08 2021 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доцент _____ Таныгин М.О.
(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № 7 «28» 02 2022 г., на заседании кафедры ИБ №11 от 30.06.2022г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № 7 «28» 02 2022 г., на заседании кафедры ИБ протокол №1 от 30.08.2023
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Мухомеев А.Н.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №___ «__»_____20___г., на заседании кафедры _____.
(наименование кафедры, дата, номер протокола)

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 преподавания дисциплины

Дисциплина "Защищённые информационные системы" изучается с целью изучения технологий, методов и средств создания защищенных информационных систем.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- сформировать профессиональную культуру обеспечения информационной безопасности (ИБ) в ИС;
- понимать принципы построения защищенных ИС;
- познакомиться с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных ИС;
- изучить подходы и методы 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.
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

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-1.3 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 проектируемую систему обеспечения информационной безопасности	***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
		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

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 компии	*наименование компетенции*		
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
		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

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 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-4.2 Составляет пошаговый план научной деятельности, 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-4.4 Создаёт технические задания и технические проекты при организации НИОКР	***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.

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 компии	*наименование компетенции*		
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-5.3 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-5.4 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
		ОПК-5.5 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 базовую часть блока 1 «Дисциплины (модули»») основной профессиональной образовательной программы – программы магистратуры 10.04.01 Информационная безопасность профиль «Защищённые информационные системы». Дисциплина изучается на 1 курсе в 1 семестре.

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 трудоёмкость (объём) дисциплины составляет 6 зачётных единиц, 216 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
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 предусмотрена
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 системы информационной безопасности	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.	Мероприятия по защите информации.	Нормативно-законодательный аспект. Процедурный аспект. Программно-технический аспект.
4.	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	Структурирование ЗИС. Анализ безопасности ИС. Критерии адекватности средств защиты**.** Структура профиля защиты ИТ-продукта. Соотношение эффективности и рентабельности систем информационной безопасности. Зависимость эффективности защиты от величины ущерба
5.	Оценочные стандарты и технические спецификации.	"Оранжевая книга" как оценочный стандарт. Стандарты информационной безопасности распределенных систем. Механизмы реализации сервисов (функций) безопасности. Администрирование средств безопасности
6.	Критерии оценки безопасности информационных технологий.	Основные понятия. Стандарт "Критерии оценки безопасности информационных технологий" . Иерархия класс-семейство-компонент-элемент. Требования доверия безопасности.
7.	Руководящие документы ФСТЭК России.	Требования к защищенности автоматизированных систем. Классы защищённости информационных систем. Аспекты защищённых ИС, фигурирующие в требованиях ФСТЭК. Классификация защищённых информационных ситсем
8.	Описание информационной системы и особенностей ее функционирования	Структура и состав информационной системы. Описание физических, функциональных, технологических и логических взаимосвязей
9.	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
10.	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.
11.	Описание угроз безопасности информации (модель угроз безопас-	Определение перечня угроз безопасности информации, возможных с учетом потенциала нарушителя. Определение перечня угроз безопасности информации, возможных с учетом

	ности информации)	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.
12.	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

Таблица 4.1.2 – Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Понятие информационной системы и рассмотрение архитектур применяемых информационных систем	2		1	У 1-5 МУ 1-4	УО, ЗПР	ОПК-1, ОПК-2
2.	Основные аспекты построения системы информационной безопасности	2	1		У 1-5 МУ 1-4	УО, ЗЛР	УК-1, ОПК-1
3.	Мероприятия по защите информации.	4	2		У 1-5 МУ 1-4	УО, ЗЛР	УК-1, ОПК-1, ОПК-2, ОПК-5
4.	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	4	3		У 1-5 МУ 1-4	УО, ЗЛР	ОПК-1, ОПК-2, ОПК-4, ОПК-5
5.	Оценочные стандарты и технические спецификации.	2		2	У 1-5 МУ 1-4	УО, ЗПР	УК-1, ОПК-1, ОПК-5
6.	Критерии оценки безопасности информационных технологий.	4			У 1-5	УО	УК-1, ОПК-1, ОПК-2
7.	Руководящие документы	2	4		У 1-5	УО, ЗЛР	УК-1,

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

С – собеседование, Т – тест, ЗЛР – защита лабораторной работы, ЗПР – защита практической работы

4.2. Лабораторные работы и практические занятия

4.2.1. Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1.	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение	6
2.	Определение показателей защищенности информации при несанкционированном доступе.	6
3.	Критерии оценки и выбора CASE-средств.	6
4.	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.	6
5.	Создание модели вероятного нарушителя	6
6.	Оценка защищённости информационной системы на основании методики ФСТЭК	6
Итого		36

4.2.2. Практические занятия

Таблица 4.2.2 – Практические занятия

№	Наименование практического занятия	Объем, час.
1.	Описание особенностей информационной системы, влияющих на её защищённость	9
2.	Соотнесение требований стандартов информационной безопасности с характеристиками информационной системы	9
3.	Описание физических и логических взаимосвязей между компонентами информационной системы. Оценка их влияния на итоговую защищённость	9
4.	Описание функциональных и технологических взаимосвязей между компонентами информационной системы	9
5.	Составление модели угроз безопасности информационной системы	9
6.	Выбор метода защиты информации	9
Итого		54

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – 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	4
2.	Основные аспекты построения системы информационной безопасности	2-3 недели	4
3.	Мероприятия по защите информации.	4-5 недели	4
4.	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	5-6 недели	5
5.	Оценочные стандарты и технические спецификации.	7-8 недели	5
6.	Критерии оценки безопасности информационных технологий.	8-9 недели	4
7.	Руководящие документы ФСТЭК России.	10-11 недели	4
8.	Описание информационной системы и особенностей ее функционирования	11-12 недели	4
9.	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя	13-14 недели	4
10.	Определение уровня защищенности данных в информационной системе	14-15 недели	4,85
11.	Описание угроз безопасности информации (модель угроз безопасности информации)	16-17 недели	5
12.	Методы выбора системы защиты информации	17-18 недели	5
Итого			52,85

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

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

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

библиотекой университета:

− библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с 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 вопросов к экзамену, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

− путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

− путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии.

Образовательные технологии.

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных и общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение в ходе лабораторных работ практикоориентированных заданий.

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

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической работы №1 «Описание особенностей информаци-	Выполнение студентом интерактивных заданий по определению этапов	4

	онной системы, влияющих на её защищённость»	проектирования информационной системы	
2.	Выполнение лабораторной работы №3 «Описание физических и логических взаимосвязей между компонентами информационной системы. Оценка их влияния на итоговую защищённость»	Выполнение студентом интерактивных заданий по определению характеристик информационной системы	6
	Итого		10

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

- целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых, их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

- применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций);

- личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения 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 Методология научных исследований Организация научной деятельности	Организация работ по обеспечению безопасности в информационных системах Управление разработкой систем безопасности	Производственная преддипломная практика
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Защищённые информационные системы	Производственная технологическая практика	
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Защищённые информационные системы	Производственная технологическая практика	
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 (научно-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 (научно-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 *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
УК - 1 / начальный	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними;	**Знает:** Основные методики осуществления критического анализа проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий. **Умеет**: Применять основные методики осуществления критического анализа проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий. **Владеет**: Навыками применения основных методик осуществления критического анализа проблемных ситуаций на основе системного подхода, вырабатывать стратегию	**Знает:** Методики осуществления критического анализа проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий. **Умеет**: Применять методики осуществления критического анализа проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий. **Владеет**: Навыками применения методик осуществления критического анализа проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	**Знает:** Современные эффективные методики осуществления критического анализа проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий. **Умеет**: Применять современные эффективные методики осуществления критического анализа проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий. **Владеет**: Навыками применения современных эффективных методик осуществления критического анализа проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		действий.		
ОПК - 1 / начальный	ОПК-1.1 Проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	**Знает:** В целом сформированные, но неполные знания возможностей и характеристик программно-технической архитектуры вычислительных сетей и комплексов, возможности современных и перспективных средств разработки программных продуктов, инструментальных сред, языков и основных концепциях прикладного и системного программирования. **Умеет:** В целом успешное, но не систематическое умение использовать программно-техническую архитектуры вычислительных сетей и комплексов, языки и инструментальные среды разработки. **Владеет:**	**Знает**: Сформированные, но содержащие отдельные пробелы знания возможностнй и характеристики программно-технической архитектуры информационных систем и комплексов, возможности современных и перспективных средств разработки программных продуктов, инструментальных сред, основных концепциях прикладного и системного программирования. **Умеет:** Успешное, но содержащее отдельные пробелы умение использовать программно-техническую архитектуры вычислительных сетей и комплексов, языки и инструментальные среды разработки.	**Знает**: Сформированные систематические знания возможностнй и характеристики программно-технической архитектуры информационных систем и комплексов, возможности современных и перспективных средств разработки программных продуктов, инструментальных сред, основных концепциях прикладного и системного программирования. **Умеет:** Успешное умение использовать программно-техническую архитектуры вычислительных сетей и комплексов, языки и инструментальные среды разработки. **Владеет:** Сформированными навыками использования программно-технической архитектуры вычисли-

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		В целом успешное, но не систематическое владение навыками использования программно-технической архитектуры вычислительных сетей и комплексов, перспективных программных продуктов, языков и инструментальных сред разработки информационных систем.	**Владеет:** Успешное, но содержащее отдельные пробелы владение навыками использования программно-технической архитектуры вычислительных сетей и комплексов, перспективных программных продуктов, языков и инструментальных сред разработки информационных систем.	тельных сетей и комплексов, перспективных программных продуктов, языков и инструментальных сред разработки.
	ОПК-1.2 Разрабатывает системы обеспечения информационной безопасности объекта	**Знать**: принципы проектирования ЗИС **Уметь**: интегрировать функциональные узлы в единую ЗИС **Владеть навыками**: организации межмодульного взаимодействия в ЗИС	**Знать**: инструментальные средства разработки ЗИС **Уметь**: выполнять работы по внедрению отдельных компонентов в многокомпонентную ЗИС **Владеть навыками**: проведения анализа технических требований к отдельным модулям проектируемой ЗИС	**Знать**: принципы декомпозиции при определении функциональности блоков разрабатываемых систем **Уметь**: анализ соответствия ункциональных возможностей компонентов ЗИС и требований политики безопасности **Владеть навыками**: формулирования требований к отдельным модулям проектируемой ЗИС
	ОПК-1.3 Планирует и оце-	**Знать**: номенклатуру организаци-	**Знать**: состав организационно-	**Знать**: назначение и правовые основы

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	нивает трудоёмкость проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений	онно-распорядительной документации, включая техническое, кадровое и финансовое обеспечение **Уметь**: сопоставлять организационно-распорядительную документацию, включая техническое, кадровое и финансовое обеспечение с функциями системы информационной безопасности; **Владеть навыками**: Работы с документацией, включая техническое, кадровое и финансовое обеспечение;	распорядительной документации, включая техническое, кадровое и финансовое обеспечение **Уметь**: сопоставлять ОРД, включая техническое, кадровое и финансовое обеспечение требованиям нормативных документов **Владеть навыками**: Формулирования отдельных положений технического, кадрового и финансового обеспечения;	отдельных положений организационно-распорядительной документации , включая техническое, кадровое и финансовое обеспечение **Уметь**: сопоставлять ОРД, включая техническое, кадровое и финансовое обеспечении, актуальной структуре ИС; **Владеть навыками**: Формирования технического, кадрового и финансового обеспечения
	ОПК-1.4 Формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании	**Знает:** Основные подходы к формированию модели угроз для автоматизированных информационных систем. **Умеет:** Оформлять и представлять мо-	**Знает:** Сформированные, но содержащие отдельные пробелы знания правил, приемов формирования модель угроз для автоматизированных информационных систем.	**Знает:** законы, технологии, правила, приемы формирования модель угроз для автоматизированных информационных систем. **Умеет:** Способен самостоятельно сформиро-

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	требований технического задания на проектируемую систему обеспечения информационной безопасности	дели угроз для автоматизированных информационных систем. **Владеет:** элементарными навыками оформления модели угроз для автоматизированных информационных систем.	**Умеет:** Способен сформировать модель угроз для автоматизированных информационных систем а. **Владеет:** основными навыками разработки защищённых информационных систем.	вать модель угроз для автоматизированных информационных систем. **Владеет:** Уверенно владеет навыками формирования требований на разрабатываемые защищённые информационные системы
	ОПК-1.5 Разрабатывает концептуальные стратегии решения задач моделирования и проектирования автоматизированных информационных систем и систем	**Знает:** Основные подходы к формированию политик информационной безопасности. **Умеет:** Оформлять и представлять результаты описания процессов протекающих в информационных системах формальным языком. **Владеет:** Описания информационных потоков в информационных системах.	**Знает:** Сформированные, но содержащие отдельные пробелы знания законов, технологий, правил, приемов обработки результатов математических экспериментов. **Умеет:** Способен обработать и представить результат проведённого анализа информационной ситсемы. **Владеет:** основными навыками теоретического анализа информационных систем на предмет защищённости.	**Знает:** Глубокие знания проблематики описания информационных процессов с точки зрения безопасности. **Умеет:** Способен самостоятельно обработать, проанализировать и представить результаты формального описания информационных систем . **Владеет:** Уверенно владеет навыками теоретического анализа информационных систем на предмет защищённости.

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ОПК - 2 / начальный	ОПК-2.1 Выбирает методы решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	**Знает:** Компоненты системы ЗИС. **Умеет:** Получать сведения о режимах работы систем передачи данных. **Владеет:** Навыками участия в сборе сведений для оценки режимов функционирования и уровня защищённости в ИС.	**Знает:** Жизненный цикл ИС **Умеет:** Организовывать реализацию жизненного цикла ЗИС. **Владеет:** Конфигурирования ЗИС для обеспечения требуемого качества и функционала.	**Знает:** Детальные аспекты жизненного цикла ИС. **Умеет:** Самостоятельно проводить оценку качества работы СЗИ **Владеет:** Навыками организации работ по вводу в эксплуатацию СЗИ
	ОПК-2.2 Разрабатывает тестовые планы и сценарии тестирования разработанного средства обеспечения информационной безопасности	**Знает:** Основные задачи анализа безопасности информационных систем. **Умеет:** С ошибками формулировать проблемные вопросы обеспечения безопасности информационных систем. **Владеет:** основными навыками создания сценарии тестирования разработанного средства обеспечения информационной безопасности.	**Знает:** Сформированные, но содержащие отдельные пробелы знания в области анализа безопасности информационных систем. **Умеет:** Способен выявлять и намечать к решению задачи, возникающие при проектировании информационных систем. **Владеет:** навыками создания сценарии тестирования разработанного средства обеспе-	**Знает:** задачи анализа безопасности информационных систем и технологии их решения. **Умеет:** Способен самостоятельно выявлять и намечать к решению задачи, возникающие при проектировании информационных систем. **Владеет:** Уверенно владеет навыками создания сценарии тестирования разработанного средства обеспечения информационной безопасности.

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
			чения информационной безопасности.	
	ОПК-2.3 Проектирует подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов	**Знает:** В целом сформированные, но неполные знания основных концепций основных концепций и технологии проектирования подсистемы безопасности информационных систем. **Умеет:** В целом успешное, но не систематическое умение использовать знания основных концепций и технологии проектирования подсистемы безопасности информационных систем сферы. **Владеет:** В целом успешное, но не систематическое владение навыков проектирования подсистемы безопасности информационных систем.	**Знает**: Сформированные, но содержащие отдельные пробелы знания основных основных концепций и технологии проектирования подсистемы безопасности информационных систем. **Умеет:** Успешное, но содержащее отдельные пробелы умение использовать знания концепций и технологии проектирования подсистемы безопасности информационных систем. **Владеет:** Успешное, но содержащее отдельные пробелы владение навыками проектирования подсистемы безопасности информационных систем.	**Знает**: Сформированные систематические знания основных концепций и технологии проектирования подсистемы безопасности информационных систем. **Умеет:** Успешное умение использовать знания полного перечня концепций и технологии проектирования подсистемы безопасности информационных систем. **Владеет:** сформированное владение навыками проектирования подсистемы безопасности информационных систем.

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	ОПК 2.4 Определяет характеристики систем защиты информации	**Знает:** Основные подходы к определению характеристики систем защиты информации. **Умеет:** Оформлять и представлять результаты процедур определения характеристики систем защиты информации. **Владеет:** элементарными навыками оформления полученных в результате экспериментов результатов.	**Знает:** Сформированные, но содержащие отдельные пробелы знания законов, технологий, правил, приемов определения характеристики систем защиты информации. **Умеет:** Способен обработать и представить результат процедур определения характеристики систем защиты информации. **Владеет:** основными навыками обработки характеристики систем защиты информации.	**Знает:** законы, технологии, правила, приемы определения характеристики систем защиты информации. **Умеет:** Способен самостоятельно определять характеристики систем защиты информации. **Владеет:** Уверенно владеет навыками обработки характеристик систем защиты информации.
ОПК - 4 / начальный	ОПК-4.2 Составляет пошаговый план научной деятельности, проводит предпроектные исследования	**Знает:** сформированные, но неполные знания о методах и приемах формализации задач, математическом аппарате и компьютерном моделировании при разработке программного обеспечения для ре-	**Знать**: Сформированные, но содержащие отдельные пробелы знания о методах и приемах формализации задач, математическом аппарате и компьютерном моделировании при проектировании	**Знать**: Сформированные систематические знания о методах и приемах формализации задач, математическом аппарате и компьютерном моделировании при проектировании защищённых информационных систем.

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		шения профессиональных задач. **Уметь:** В целом успешное, но не систематическое умение обосновать выбор математического аппарата, провести компьютерное моделирование при проектировании защищённых информационных систем. **Владеть:** В целом успешные, но не систематические навыки выбора и применения математического аппарата, проведения компьютерного моделирования при проектировании защищённых информационных систем.	защищённых информационных систем. **Уметь:** Успешное, но содержащее отдельные пробелы умение обосновать выбор математического аппарата, провести компьютерное моделирование при проектировании защищённых информационных систем. **Владеть:** Успешные, но содержащее отдельные пробелы навыки выбора и применения математического аппарата, проведения компьютерного моделирования при проектировании защищённых информационных систем	**Уметь:** Успешное умение обосновать выбор математического аппарата, провести компьютерное моделирование при проектировании защищённых информационных систем. **Владеть:** Сформированные навыки выбора и применения математического аппарата, проведения компьютерного моделирования при проектировании защищённых информационных систем.
	ОПК-4.4 Создаёт технические задания и технические проекты при организации НИОКР	**Знает:** сформированные, но неполные знания о методах и приемах формализации подзадач при проведении	**Знает** Сформированные, но содержащие отдельные пробелы знания о методах и приемах формализации	**Знает**: Сформированные систематические знания о методах и приемах формализации и описания подзадач при проведе-

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		ОКР. **Умеет:** В целом успешное, но не систематическое умение обосновать выбор этапов проведения ОКР. **Владеет:** В целом успешные, но не систематические навыки выбора этапов проведения ОКР.	подзадач при проведении ОКР. **Умеет:** Успешное, но содержащее отдельные пробелы умение обосновать выбор этапов и их содержания при проведении ОКР. **Владеет:** Успешные, но содержащее отдельные пробелы навыки выбора выбор этапов и их содержания при проведении ОКР	нии ОКР. **Умеет:** Успешное умение обосновать выбор этапов и их содержания при проведении ОКР. **Владеет:** Сформированные навыки выбора выбор этапов и их содержания при проведении ОКР.
ОПК - 5 / начальный	ОПК-5.3 Формализует задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструментальные средства анализа безопасности	**Знает:** Основные задачи анализа безопасности информационных систем. **Умеет:** С ошибками формулировать проблемные вопросы обеспечения безопасности информационных систем. **Владеет:** основными навыками формулировки проблемных вопросов обеспечения безопасности ин-	**Знает:** Сформированные, но содержащие отдельные пробелы знания в области анализа безопасности информационных систем. **Умеет:** Способен выявлять и намечать к решению задачи, возникающие при проектировании информационных систем. **Владеет:** навыками формулировки про-	**Знает:** задачи анализа безопасности информационных систем и технологии их решения. **Умеет:** Способен самостоятельно выявлять и намечать к решению задачи, возникающие при проектировании информационных систем. **Владеет:** Уверенно владеет навыками формулировки проблемных вопросов обеспечения безопасности

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		формации.	блемных вопросов обеспечения безопасности информации..	информации..
	ОПК-5.4 Представляет результаты, полученные в ходе выполнения научно-исследовательского проекта грамотно, лаконично, в достаточном объеме на русском и иностранном языках	**Знает:** Базовые стандарты оформления технических и научных текстов. **Умеет:** Аннотировать этапы работ по обеспечению информационной безопасности. **Владеет:** элементарными навыками аннотирования работ по обеспечению информационной безопасности.	**Знает:** Знает стандарты и нормативы оформления технической и проектной документации. **Умеет:** подробно описывать этапы работ по обеспечению информационной безопасности. . **Владеет:** Навыками описания работ по обеспечению информационной безопасности.	**Знает:** Стандарты, правила и особенности стиля речи научных и технических текстов. **Умеет:** вариативно описывать этапы работ по обеспечению информационной безопасности. **Владеет:** Навыками формирования различных текстов для описания работ по информационной безопасности.
	ОПК-5.5 Применяет в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследований	**Знает:** базовые знания в области экспериментального исследования защищенности объектов **Умеет:** Аннотировать этапы работ по экспериментальным исследованиям защищенности объектов **Владеет:**	**Знает:** сформированные, но содержащие отдельные пробелы знания в области экспериментального исследования защищенности объектов **Умеет:** Проводить экспериментальные исследования защищенности объектов с применением со-	**Знает:** методы экспериментального исследования защищенности объектов **Умеет:** Проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и про-

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		элементарными навыками аннотирования работ по апробации и внедрению разработанных эффективных технологий	ответствующих физических и математических методов **Владеет:** Навыками описания работ по апробации и внедрению разработанных эффективных технологий	граммных средств обработки результатов эксперимента **Владеет:** Навыками апробации и внедрения разработанных эффективных технологий

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

Таблица 7.3 – Паспорт комплекта оценочных средств

№ 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	ОПК-1, ОПК-2	Лекция, СРС, практическая работа	ВУО КВЗПР	1-7 1-5	Согласно табл. 7.2
2.	Основные аспекты построения системы	УК-1, ОПК-1	Лекция, СРС, лабораторная	ВУО КВЗЛР	1-9 1-5	Согласно табл. 7.2

1	2	3	4	5	6	7
	информационной безопасности		работа			
3.	Мероприятия по защите информации.	УК-1, ОПК-1, ОПК-2, ОПК-5	Лекция, СРС, лабораторная работа	ВУО КВЗЛР	1-10 1-5	Согласно табл. 7.2
4.	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, лабораторная работа	ВУО КВЗЛР	1-7 1-5	Согласно табл. 7.2
5.	Оценочные стандарты и технические спецификации.	УК-1, ОПК-1, ОПК-5	Лекция, СРС, практическая работа	ВУО КВЗПР	1-7 1-5	Согласно табл. 7.2
6.	Критерии оценки безопасности информационных технологий.	УК-1, ОПК-1, ОПК-2	Лекция, СРС,	ВУО	1-5	Согласно табл. 7.2
7.	Руководящие документы ФСТЭК России.	УК-1, ОПК-1, ОПК-2	Лекция, СРС, лабораторная работа	ВУО КВЗЛР	1-5 1-5	Согласно табл. 7.2
8.	Описание информационной системы и особенностей ее функционирования	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, практическая работа	ВУО КВЗПР	1-5 1-5	Согласно табл. 7.2
9.	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя	УК-1, ОПК-1, ОПК-2, ОПК-4,	Лекция, СРС, лабораторная работа	ВУО КВЗЛР	1-5 1-5	Согласно табл. 7.2
10.	Определение уровня защищенности данных в информационной системе	ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, лабораторная работа	ВУО КВЗЛР	1-5 1-5	Согласно табл. 7.2
11.	Описание угроз безопасности информации (модель угроз безопасности информации)	УК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, практическая работа	ВУО КВЗПР	1-5 1-5	Согласно табл. 7.2
12.	Методы выбора системы защиты информации	УК-1, ОПК-2, ОПК-4, ОПК-5	Лекция, СРС, практическая работа	ВУО КВЗПР	1-5 1-5	Согласно табл. 7.2

ВУО- вопросы для устного опроса

КВЗПР- контрольные вопросы для защиты практической работы

КВЗЛР- контрольные вопросы для защиты лабораторной работы

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по теме 6 «Критерии оценки безопасности информационных технологий»

1. Опишите иерархию сущностей в "Критериях оценки безопасности информационных технологий".
2. Назовите основные термины, описанные в "Критериях оценки безопасности информационных технологий".
3. Опишите структуру класса «приватность».
4. Опишите структуру класса «использование ресурсов».
5. Что такое требования доверия безопасности и для чего они нужны?

Контрольные вопросы для защиты лабораторной работы 4 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»

1. Для чего служит Доктрина информационной безопасности?
2. Что выступает в качестве средств защиты информации, подлежащих сертификации в Системе сертификации средств защиты информации по требованиям безопасности информации?
3. Основные схемы сертификации средств защиты информации.
4. Какие функции осуществляет ФСТЭК России в пределах своей компетенции?

Контрольные вопросы для защиты практической работы 2 «Соотнесение требований стандартов информационной безопасности с характеристиками информационной системы»

1. Какие функции выполняют стандарты в области информационной безопасности?
2. Основные области стандартизации информационной безопасности.
3. Классификации стандартов информационной безопасности.
4. Какие процедуры должны быть выполнены разработчиком при разработке средства?
5. Что должно предусматривать проектирование средства, соответствующего шестому уровню доверия?

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в виде компьютерного тестирования.

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.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) 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.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Отметьте методы сбора информации при проведении обследования объекта автоматизации.

1) анкетирование
2) интервьюирование
3) метод аналогий

4) создание "фотографии рабочего дня"
5) метод проб и ошибок
6) метод Монте-Карло

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

Компетентностно-ориентированная задача:

Для некоторой системы характерно наличие проводного канала связи (витой пары), соединяющей компьютеры, находящиеся в аттестованных помещениях. Витая пара проходит через неаттестованное помещение. Предложите перечень мероприятий, направленных на сохранения класса защиты данной информационной системы.

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»;

– 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
Выполнение лабораторной работы №1 «Описание случайного процесса с помощью аппарата цепей Маркова»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение лабораторной работы №2 «Аналитическое получение характеристик моделируемых систем»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение лабораторной работы №3 «Получение характеристик моделируемых систем численными методами»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение лабораторной работы №4 «Анализ точности вычислений»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение лабораторной работы №5 «Исследование тупиковых ситуаций»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение лабораторной работы №6 «Моделирование процесса передачи данных»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение практической работы №1 «Описание случайного процесса с помощью аппарата цепей Маркова»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»

Выполнение практической работы №2 «Аналитическое получение характеристик моделируемых систем»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение практической работы №3 «Получение характеристик моделируемых систем численными методами»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение практической работы №4 «Анализ точности вычислений»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение практической работы №5 «Исследование тупиковых ситуаций»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение практической работы №6 «Моделирование процесса передачи данных»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Устный опрос по темам 1-12	12	Доля правильных ответов 50-90%	24	Доля правильных ответов более 90%
Компетентностные задачи	0		6	
ИТОГО	24		48	
Посещаемость	0		16	
Экзамен	0		36	
ИТОГО	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2балла,
- 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 за тестирование –36 баллов.

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

8.1 Основная литература

1. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин :Директ-Медиа, 2021. – 210 с. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

2. Марухленко, А. Л. Разработка защищённых интерфейсов Web-приложений : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва ; Берлин : Директ-Медиа, 2021. – 175 с. – URL: https://biblioclub.ru/index.php?page=book&id=599050 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная литература

3. Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский ; Новосибирский государственный технический университет. - Новосибирск : Новосибирский государственный технический университет, 2018. - 80 с. - URL: http://biblioclub.ru/index.php?page=book&id=576354 (дата обращения: 16.02.2023) . - Режим доступа: по подписке. – Текст: электронный.

4. Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко и др. – Москва ; Берлин : Директ-Медиа, 2021. – 201 с. – URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

5. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

8.3 Перечень методических указаний

1) Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Электрон. текстовые дан. (541 КБ). - Курск : ЮЗГУ, 2017. - 16 с. : ил., табл. - Библиогр.: с. 16. - Б. ц.

2) Определение показателей защищенности информации при несанкционированном доступе [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Электрон. текстовые дан. (342 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

3) Критерии оценки и выбора CASE-Средств : методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Электрон. текстовые дан. (298 КБ). - Курск : ЮЗГУ, 2022. - 11 с. - Загл. с титул. экрана. - Б. ц.

4) Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Электрон. текстовые дан. (324 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Облачный сервис математических вычислений SMath Studio in the Cloud [официальный сайт]. Режим доступа: https://ru.smath.com/cloud/

2) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru

3) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/

4) Общероссийский портал Math-Net.Ru [официальный сайт]. Режим доступа: http://www.mathnet.ru/

5) База данных "Патенты России"

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Математическое моделирование технических объектов и систем управления» являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; за- крепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному 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.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и

практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Математическое моделирование технических объектов и систем управления»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

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 усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Математическое моделирование технических объектов и систем управления» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Математическое моделирование технических объектов и систем управления» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385, откры-

тая среда разработки программного обеспечения Lazarus (Свободное ПО http://www.lazarus.freepascal.org/)

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+

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 присут-

ствие 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			