Аннотация к рабочей программе дисциплины «Управление разработкой систем безопасности»

Цель преподавания дисциплины

Целью преподавания дисциплины "Управление разработкой систем безопасности" является ознакомление студентов с основными способами, методами, принципами, технологиями и средствами управления, проектирования, создания и модернизации защищённых телекоммуникационных систем и сетей.

Задачи изучения дисциплины

– изучение основных методов и способов защиты информации, передаваемой в информационных системах и сетях, а также основных принципов, используемых при организации и проведении мероприятий по защите информации на объектах защиты;

– изучение принципов работы и основных технических характеристик средств защиты информации, передаваемой в информационных системах и сетях;

– овладение навыками по разработке, проектированию и модернизации защищённых информационных систем;

– овладение навыками проведения теоретических и экспериментальных исследований защищённости информационных систем;

– овладение навыками организации, планирования и управления коллективами по созданию защищённых информационных систем;

– овладение навыками управления персоналом, обслуживающим защищённые информационные системы;

– изучение обязанностей персонала по разработке и обслуживанию информационных систем;

– изучение задач при проведении работ по развитию, модернизации защищённой информационной системы;

– анализ требований, предъявляемых к программным, программно-аппаратным и техническим средствам, и системам защиты информации;

– изучение эксплуатационной документации и овладение навыками проведения процедур сертификации и аттестации средств и систем защиты и объектов информатизации;

– изучение основных нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации;

– овладение навыками управления проектом на всех этапах его жизненного цикла.

Компетенции, формируемые в результате освоения дисциплины

Способен управлять проектом на всех этапах его жизненного цикла. (УК-2);

Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки образования в течение всей жизни (УК-6);

Способен оценивать эффективность механизмов безопасности в телекоммуникационных системах и сетях (ПК-3);

Способен формировать проектные решения по созданию и модернизации телекоммуникационных систем и сетей в защищенном исполнении (ПК-4).

Разделы дисциплины

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

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

_____М.О. Таныгин
(подпись, инициалы, фамилия)

«_31_» _____08_____ 20_21_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление разработкой систем безопасности

(наименование дисциплины)

ОПОП ВО 10.05.02Информационная безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))
телекоммуникационных систем

направленность (профиль, специализация) «Управление безопасностью
наименование направленности (профиля, специализации)
телекоммуникационных систем и сетей»

форма обучения _____очная_____
(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины Управление разработкой систем безопасности составлена в соответствии с ФГОС ВО – специалитет специальности 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специальность Управление безопасностью телекоммуникационных систем и сетей, одобренного Ученым советом университета (протокол №6 «26» 02 2021 г.).

Рабочая программа дисциплины Управление разработкой систем безопасности обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специальность Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности Протокол №1 «30» 06 2021 г.

Зав. кафедрой Таныгин М.О.
Разработчик программы
к.воен.н., доцент ХанисА.Л.
Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Управление разработкой систем безопасности пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специальность Управление безопасностью телекоммуникационных систем и сетей, одобренного Ученым советом университета Протокол № «6» 26.02 2021г., на заседании кафедры ИБ, протокол №11 от 30.06.2022 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой М.О. Таныгин

Рабочая программа дисциплины Управление разработкой систем безопасности пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специальность Управление безопасностью телекоммуникационных систем и сетей, 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 дисциплины

Целью преподавания дисциплины "Управление разработкой систем безопасности" является ознакомление студентов с основными способами, методами,принципами, технологиями и средствами управления,проектирования, создания и модернизациизащищённых телекоммуникационных систем и сетей.

1.2 Задачи дисциплины

- изучение основных методов испособов защиты информации, передаваемойвинформационных системах и сетях, а также основных принципов, используемых при организации и проведении мероприятий по защите информации на объектах защиты;
- изучение принципов работы и основных технических характеристик средств защиты информации, передаваемой в информационных системах и сетях;
- овладение навыками по разработке, проектированию и модернизации защищённых информационных систем;
- овладение навыкамипроведения теоретических и экспериментальных исследований защищённости информационных систем;
- овладение навыками организации, планирования и управления коллективами по созданию защищённых информационных систем;
- овладение навыками управления персоналом, обслуживающим защищённые информационные системы;
- изучение обязанностей персонала по разработке и обслуживанию информационных систем;
- изучение задач при проведении работ по развитию, модернизации защищённой информационной системы;
- анализ требований, предъявляемых к программным, программно-аппаратным и техническим средствам и системам защиты информации;
- изучение эксплуатационной документации и овладение навыкамипроведения процедур сертификации и аттестации средств и систем защиты и объектов информатизации;
- изучение основных нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации;
- овладение навыкамиуправления проектом на всех этапах его жизненного цикла.

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

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*		
УК-2	Способен управлять проектом на всех этапах его жизненного цикла.	УК-2.3 Планирует необходимые ресурсы, в том числе с учетом их заменимости.	***Знать:*** требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру, архитектуру и состав типовых телекоммуникационных систем и сетей (ТКС), этапы разработки типовой ТКС, сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем. ***Уметь***: организовать выполнение работ в рамках проекта по разработке телекоммуникационных систем и сетей, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов, своевременно вносить коррективы в разработанную документацию и устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта. ***Владеть:*** навыками планирования и организации выполнения работ в рамках проектов по разработке телекоммуникационных систем и сетей, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других

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*		
			нормативных и юридических документов; своевременного внесения корректив в разработанную документацию и устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов.
		УК-2.5 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта.	***Знать:*** требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру и архитектуру и состав типовых ТКС, этапы разработки типовой ТКС, сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем. ***Уметь***: организовать и контролировать выполнение работ в рамках проекта по разработке ТКС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов, своевременно вносить коррективы в разработанную документацию и устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта. ***Владеть:*** навыками организации выполнения работ в рамках проектов по разработке ТКС, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов; своевременного

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*		
			внесения корректив в разработанную документацию и устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов.
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценкии образования в течение всей жизни.	УК-6.1 Использует инструменты и методы управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей.	***Знать:*** классификацию программно-аппаратных и телекоммуникационных средств защиты, технические характеристики и возможности сетевого оборудования инфо-коммуникационных сетей, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности систем и сетей, основные действующие нормативные документы и юридические законы в области защиты информации. ***Уметь:*** проводить анализ защищенности локальной вычислительной сети, настраивать режимы работы межсетевых экранов, проводить анализ информационных рисков, определять оптимальный состав программных и аппаратных средств для построения инфо-коммуникационных сетей, применять действующие нормативные документы и юридические законы в области защиты информации. ***Владеть:*** навыками выбора программно-аппаратных средств и телекоммуникационного оборудования, эксплуатации программных средств анализа и управления рисками, навыками разработки защищенных сайтов, разработки и установки программных средств защиты инфо-коммуникационных сетей, определения действующих нормативных требований и юридических законов в области защиты информации.

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*		
ПК-3	Способен оценивать эффективность механизмов безопасности в телекоммуникационных системах и сетях.	ПК-3.1 Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.	***Знать:***требования действующих стандартов и рекомендаций, определяющих критерии оценки безопасности ТКС и этапы анализа рисков и угроз безопасности и уязвимости ТКС; классификацию общих критериев, пути организации общих критериев; требования к разработке должностных инструкций; порядок эксплуатации программно-аппаратных средств защиты ТКС; основные принципы построения политики безопасности;методы и способы защиты информации в ТКС, методы анализа угроз и оценки рисков информационной безопасности ТКС, методы и методики оценки эффективности СЗИ. ***Уметь:*** применять требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС; разрабатывать служебную и техническую документацию; применять средства защиты информации в соответствии с заданными требованиями к ТКС; проводить анализ информационных рисков, методы и модели оценки функционирования программно-аппаратных средств защиты информации. ***Владеть:*** навыками применения требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС; разработки служебной и технической документации; программных средств защиты информации, разработки архитектуры сетевой защиты, методами, методиками и моделями оценки функционирования программно-аппаратных средств защиты информации.
		ПК-3.2 Оценивает соответствие	***Знать***: технические характеристики и особенности функционирования программно-аппаратных средств ЗИ в

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*		
		механизмов безопасности системы требованиям нормативных документов и рискам.	телекоммуникационных системах исетях; перечень и объём мероприятий по обеспечению безопасности и защищённости ТКС, виды угроз ТКС, типы, виды, назначение средств защиты информации в ТКС; состав, характеристики, назначение, функции оборудования ТКС; классификацию антивирусного ПО, способы настройки сетевых экранов. ***Уметь:*** проводить анализ угроз, рисков ТКС, осуществлять выбор оборудования и средств защиты ТКС в соответствии с решаемыми ТКС задачами, классифицировать средства защиты исходя из функционала ТКС, определять состав средств защиты для обеспечения выполнения задач ТКС; применять программные средства защиты сетевого оборудования, антивирусные программные комплексы, настраивать режимы работы межсетевых экранов. ***Владеть:***навыками анализа функциональных возможностей оборудования и средств защиты ТКС, технических характеристик сетевого оборудования и программно-аппаратных средств ЗИ в ТКС; выбора и эксплуатации средств ЗИ в ТКС в соответствии с функциональными задачами ТКС, настройки сетевых экранов, установки ПО, разработки защищённых сайтов.
		ПК-3.3 Формулирует критерии оценки эффективности механизмов безопасности, используемых в телекоммуника	***Знать:***требования действующих стандартов и рекомендаций, определяющих критерии оценки эффективности механизмов безопасности телекоммуникационных систем и этапы анализа рисков и угроз безопасности и уязвимости ТКС; классификацию общих критериев, пути организации общих критериев; требования к разработке должностных инструкций; порядок

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*		
		ционных системах.	эксплуатации программно-аппаратных средств защиты ТКС; основные принципы построения политики безопасности;методы и способы защиты информации в ТКС, методы анализа угроз и оценки рисков информационной безопасности ТКС. ***Уметь:*** применять требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС; разрабатывать служебную и техническую документацию; применять средства защиты информации в соответствии с заданными требованиями к ТКС; проводить анализ информационных рисков и эффективности, применяемых СЗИ в ТКС. ***Владеть:*** навыками применения требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС; разработки служебной и технической документации; программных средств защиты информации, разработки архитектуры сетевой защиты, анализа информационных рисков и эффективности, применяемых СЗИ в ТКС.
		ПК-3.4 Формулирует предложения по повышению эффективности механизмов безопасности, используемых в телекоммуникационных системах.	***Знать:*** классификацию, назначение, конфигурацию, состав, структуру, принципы функционирования типовых телекоммуникационных систем предприятий и организаций; основы управления ТКС; виды, состав, назначение, принципы функционирования, функции и взаимосвязь основных элементов и компонентов ТКС; понятие, типы, примеры архитектур ТКС, принципы работы ТКС; типовые архитектуры ТКС с точки зрения программно-аппаратной реализации; классификацию архитектур, распределённые системы; особенности

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*		
			проектирования распределённых систем; методы и средства защиты информации в ТКС, способы защиты информационных систем, методы анализа угроз и оценки рисков информационной безопасности ТКС. ***Уметь:*** проводить сравнительный анализ состава, технических характеристик, решаемых задач компонентов ИС прикладного характера, системного и прикладного ПО, обеспечивающего функционирование ТКС; оценку вариантов предлагаемых к реализации архитектур ТКС; выбор наиболее оптимального варианта построения предлагаемой архитектуры ТКС; формировать требования к структуре ТКС исходя из решаемых задач; разрабатывать регламентирующие документы для принятия решения на технических совещаниях; предложения для технических советов с обоснованием выбора предлагаемой архитектуры прикладной ТКС. ***Владеть:*** навыками сравнительного анализа технических средств и оборудования из состава телекоммуникационных систем, оценки предлагаемых к реализации вариантов построения телекоммуникационных систем, выбора оптимальной архитектуры прикладной ТКС исходя из решаемых системой задач, разработки и оформления документов и предложений по повышению эффективностиприменения средств безопасности телекоммуникационных систем.
ПК-4	Способен формировать проектные решения по созданию и модернизации	ПК-4.1 Разрабатывает проектные документы на средства	***Знать***: сетевой график проведения работ в рамках проекта, технологический цикл проведения разработок, состав материально технической и лабораторной базы необходимой для разработки

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*		
	телекоммуникационных систем и сетей в защищенном исполнении.	защиты информации создаваемых телекоммуникационных систем и сетей.	программно-аппаратных средств, сборки и монтажа сетевого оборудования ТКС; порядок разработки и согласования расчётно-калькуляционных материалов проекта по разработке ТКС, знать состав и структуру планово-хозяйственных документов, финансовых документов, отчётных документов, порядок их оформления, программные продукты и системы управления хозяйственной деятельностью. ***Уметь:*** управлять материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию ТКС. ***Владеть:*** навыками управления и распределения материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию ТКС.
		ПК-4.2 Готовит техническую и проектную документацию по вопросам создания и эксплуатации телекоммуникационных систем и сетей.	***Знать:***порядок внедрения, отладки и развития процессов и этапов разработки требований, задач, критериев качества и методов обеспечения информационной безопасности защищённых ТКСв процессе их эксплуатации и модернизации. ***Уметь:***организоватьи управлять внедрением, отладкой и развитиемпроцессов и этапов работ, методов обеспечения информационной безопасности защищённых ТКСв процессе их эксплуатации и модернизации. ***Владеть:***навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки системобеспечения информационной безопасности ТКСв процессе их эксплуатации и модернизации.

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*		
		ПК-4.3 Проводит аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации.	***Знать:*** виды угроз и возможные каналы утечки информации, основные принципы построения политики информационной безопасности, основные виды сетевых атак и методы противодействия им, требования к средствам защиты информации и защищённым системам и сетям, технические характеристики, особенности установки и функционирования программных средств и комплексов защиты телекоммуникационных сетей и систем, средства разработки алгоритмов функционирования СЗИ ТКС. ***Уметь:*** применятьметоды и способы разработки алгоритмов, программных средств и комплексов защиты информации в ТКС, эксплуатировать антивирусные программные комплексы, снижать вероятность отрицательных последствий сетевых атак путем правильной настройки операционной системы, применять средства защиты информации для решения практических задач в области информационной безопасности, проводить анализ алгоритмов и программных средств защиты информации на предмет соответствия требованиям защищённых ТКС. ***Владеть:*** навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры инфо-коммутационных систем и сетевой защиты, поиска и обнаружения уязвимых узлов инфо-коммуникационных систем и сетей, анализа алгоритмов и программных средств защиты информации на предмет соответствия требованиям защищённых ТКС,разработки алгоритмов, программных средств и комплексов защиты информации в ТКС.
		ПК-4.4	***Знать:*** номенклатуру современных

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*		
		Производит сравнительный анализ вариантов конфигураций и состава телекоммуникационных систем и сетей.	программно-аппаратных средств телекоммуникационных систем и сетей;назначение, организацию и принципы функционировании программно-аппаратных средств ТКС;механизмы защиты программно-аппаратных средств ТКС; классификацию и архитектуру ТКС; основные этапы аудита безопасности информационных систем; методы анализа и управления рисками; основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем; основные этапы сравнительного анализа состава и конфигурации ТКС, в том числе номенклатуру покупных и вновь разрабатываемых программных и аппаратных средства ТКС.

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*		
			Уметь: устанавливать современные программные средства, подключать аппаратные средства ТКС; настраивать операционные системы и их подсистемы; сопоставлять структурную организацию программных и аппаратных средств требованиям политики безопасности; проводить анализ угроз, рисков, применять антивирусные программные комплексы, настраивать режимы работы межсетевых экранов, проводить анализ защищенности локальной вычислительной сети, проводить анализ информационных рисков; проводить основные этапы сравнительного анализа состава и конфигурации ТКС, в том числе покупных и вновь разрабатываемых программных и аппаратных средств ТКС. ***Владеть:*** навыками применения программно-аппаратных средств; реализации требуемых политик безопасности с помощью современных программно-аппаратных средств защиты информации; проведения проверок работоспособности и эффективности применения программно-аппаратных средств, защиты информации в компьютерных системах, анализа защищенности ТКС, эксплуатации программных и аппаратных средств; проведения основных этапов сравнительного анализа состава и конфигурации ТКС, в том числе покупных и вновь разрабатываемых программных и аппаратных средств ТКС.

2. Указание места дисциплины в структуре основной профессиональнойобразовательной программы

Дисциплина «Управление разработкой систем безопасности», входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули») основной профессиональной образовательной программы – программы специалитета(магистратуры,бакалавриата) 10.05.02Информационная безопасностьтелекоммуникационных систем, направленностьУправление безопасностью телекоммуникационных систем и сетей.Дисциплина изучается на 5 курсе в 9 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 трудоемкость (объем) дисциплины составляет 6 зачетных единиц (з.е.), 216академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	216
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	90
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	2	3

1	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
2	Мероприятия по защите информации.	Нормативно-законодательный аспект. Процедурный аспект. Программно-технический аспект.
3	Требования к архитектуре ТКС для обеспечения безопасности ее функционирования.	Структурирование ЗТКС. Анализ безопасности ТКС. Критерии адекватности средств защиты**.** Структура профиля защиты ИТ-продукта. Соотношение эффективности и рентабельности систем информационной безопасности. Зависимость эффективности защиты от величины ущерба.
4	Оценочные стандарты и технические спецификации.	"Оранжевая книга" как оценочный стандарт. Стандарты информационной безопасности распределенных систем. Механизмы реализации сервисов (функций) безопасности. Администрирование средств безопасности.
5	Критерии оценки безопасности информационных технологий.	Основные понятия. Стандарт "Критерии оценки безопасности информационных технологий" . Иерархия класс-семейство-компонент-элемент. Требования доверия безопасности.
6	Руководящие документы ФСТЭК России.	Требования к защищенности автоматизированных систем. Классы защищённости информационных систем. Аспекты защищённых ТКС, фигурирующие в требованиях ФСТЭК. Классификация защищённых информационных систем.

Таблица 4.1.2 - Содержание дисциплины и ее 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	Основные аспекты построения системы информационной безопасности.	6	-	1	У-1,3, МУ-1	УО – 2, ЗПР – 2	УК-2, УК-6, ПК-3, ПК-4
2	Мероприятия по защите информации.	6	-	2	У-1-3, МУ-2	УО –4, ЗПР – 4	УК-2, УК-6, ПК-3, ПК-4
3	Требования к	6	-	3		УО-8,	

	архитектуре ИС для обеспечения безопасности ее функционирования.				У-4,5, МУ-3	ЗПР - 8	УК-2, УК-6, ПК-3, ПК-4
4	Оценочные стандарты и технические спецификации.	6	1	-	У-1,6,7, МУ-5	УО – 12, ЗЛР – 12	УК-2, УК-6, ПК-3, ПК-4
5	Критерии оценки безопасности информационных технологий.	6	2	-	У-1,2, МУ-6	УО-14, ЗЛР – 14	УК-2, УК-6, ПК-3, ПК-4
6	Руководящие документы ФСТЭК России.	6	3	4	У-4,5 МУ-4, МУ-7	УО – 18, ЗПР – 16,18, ЗЛР – 16,18	УК-2, УК-6, ПК-3, ПК-4
	Всего	36	36	54			

УО – устный опрос, ЗЛР – защита лабораторной работы, ЗПР – защита практической работы

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.3 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1.	Лабораторная работа №1 – Разработка проекта локальной вычислительной сети предприятия	12
2.	Лабораторная работа №2 – Устранение уязвимостей сетевых портов	12
3.	Лабораторная работа №3 – Изучение механизмов безопасности сетей Wi-Fi	12
Итого		36

4.2.2Практические занятия

Таблица 4.2.1–Практические занятия

№п/п	Наименование практической работы	Объем, час.
1	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение.	12
2	Определение показателей защищенности информациипри несанкционированном доступе.	14
3	Критерии оценки и выбора CASE-средств.	14
4	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.	14

Итого	54

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Основные аспекты построения системы информационной безопасности.	2 неделя	9
2	Мероприятия по защите информации.	3 неделя	8,85
3	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	4 неделя	9
4	Оценочные стандарты и технические спецификации.	5 неделя	8
5	Критерии оценки безопасности информационных технологий.	6 неделя	9
6	Руководящие документы ФСТЭК России.	7 неделя	9
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 за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путемразработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачёту;

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

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. 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 профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

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

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
1	Лабораторная работа №1. Разработка проекта локальной вычислительной сети предприятия.	Анализ конкретных ситуаций	2
2	Лабораторная работа №2. Устранение уязвимостей сетевых портов.	Анализ конкретных ситуаций	2
3	Лабораторная работа №3. Изучение механизмов безопасности сетей Wi-Fi.	Анализ конкретных ситуаций	

4	Практическая работа №1. Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение.	Анализ конкретных ситуаций	2
5	Практическая работа№2. Определение показателей защищенности информации при несанкционированном доступе.	Анализ конкретных ситуаций	2
6	Практическая работа №3.Критерии оценки и выбора CASE-средств.	Анализ конкретных ситуаций	2
Итого			12

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
УК-2. Способен управлять проектом на всех этапах его жизненного цикла.	Экономическое обоснование проектных решений.	Экономическое обоснование проектных решений. Управление информационной безопасностью телекоммуникационных систем.	Подготовка к процедуре защиты и защита выпускной квалификационной работы.
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и	Введение в специальность и планирование профессиональной карьеры.	Подготовка к процедуре защиты и защита выпускной квалификационной работы.	Подготовка к процедуре защиты и защита выпускной квалификационной работы.

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
ПК-3. Способен оценивать эффективность механизмов безопасности в телекоммуникационных системах и сетях.	Методы и средства пространственного анализа.	Методы и средства пространственного анализа. Методы пространственного моделирования радиоканала.	Методы и средства пространственного анализа. Методы пространственного моделирования радиоканала. Производственная проектно-
ПК-4. Способен формировать проектные решения по созданию и модернизации телекоммуникационных систем и сетей в защищенном		Производственная проектно-технологическая практика.	Производственная проектно-технологическая практика. Подготовка к процедуре защиты и защита выпускной квалификационной работы.

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

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5

УК-2, завершающий.	УК-2.3 Планирует необходимые ресурсы, в том числе с учетом их заменимости.	Знать: требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру, архитектуру и состав типовых телекоммуникационных систем и сетей (ТКС). Уметь: организовать выполнение работ в рамках проекта по разработке телекоммуникационных систем и сетей. Владеть: навыками планирования и организации выполнения работ в рамках проектов по разработке телекоммуникационных систем и сетей.	Знать: этапы разработки типовой ТКС, сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы. Уметь: контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов. Владеть: навыками контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов.	Знать: требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем. Уметь: своевременно вносить коррективы в разработанную документацию и устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта. Владеть: Навыками своевременного внесения корректив в разработанную документацию и устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов.
	УК-2.5 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнител	Знать: требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения	Знать: этапы разработки типовой ТКС, сетевой график выполнения проекта, должностные	Знать: показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности

	ьные изменения в план реализации проекта, уточняет зоны ответственности участников проекта.	работ по проекту, классификацию, номенклатуру и архитектуру и состав типовых ТКС. Уметь: организовать и контролировать выполнение работ в рамках проекта по разработке ТКС. Владеть: навыками организации выполнения работ в рамках проектов по разработке ТКС.	обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации. Уметь: контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов. Владеть: навыками контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов.	автоматизированных систем. Уметь: своевременно вносить коррективы в разработанную документацию и устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта. Владеть: Навыками своевременного внесения корректив в разработанную документацию и устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов.
УК-6, завершающий.	УК-6.1 Использует инструменты и методы управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей.	Знать: классификацию программно-аппаратных и телекоммуникационных средств защиты, технические характеристики и возможности сетевого оборудования инфо-коммуникационных сетей. Уметь:	Знать: каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, показатели защищенности средств вычислительной техники от несанкционированного доступа. Уметь:	Знать: классы защищенности систем и сетей, основные действующие нормативные документы и юридические законы в области защиты информации. Уметь: применять действующие нормативные

	.	проводить анализ защищенности локальной вычислительной сети, настраивать режимы работы межсетевых экранов. Владеть: навыками выбора программно-аппаратных средств и телекоммуникационного оборудования.	проводить анализ информационных рисков, определять оптимальный состав программных и аппаратных средств для построения ТКС. Владеть: навыками эксплуатации программных средств анализа и управления рисками, навыками разработки защищенных сайтов, разработки и установки программных средств защиты инфо-коммуникационных сетей.	документы и юридические законы в области защиты информациием. Владеть: навыками определения действующих нормативных требований и юридических законов в области защиты информации.
ПК-3, завершающий.	ПК-3.1 Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.	Знать: требования действующих стандартов и рекомендаций, определяющих критерии оценки безопасности ТКС и этапы анализа рисков и угроз безопасности и уязвимости ТКС. Уметь: применять требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС. Владеть навыками: навыками применения требования	Знать: классификацию общих критериев, пути организации общих критериев; требования к разработке должностных инструкций; порядок эксплуатации программно-аппаратных средств защиты ТКС. Уметь: разрабатывать служебную и техническую документацию; применять средства защиты информации в соответствии с заданными требованиями к ТКС. Владеть навыками:	Знать: основные принципы построения политики безопасности; методы и способы защиты информации в ТКС, методы анализа угроз и оценки рисков информационной безопасности ТКС, методы и методики оценки эффективности СЗИ. Уметь: проводить анализ информационных рисков, методы и модели оценки функционирования программно-аппаратных средств защиты информации. Владеть навыками: разработки

	ПК-3.2 Оценивает соответствие механизмов безопасности и системы требованиям нормативных документов и рискам. ПК-3.3 Формулирует критерии оценки эффективности механизмов безопасности, используем	действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС. Знать: технические характеристики и особенности функционирования программно-аппаратных средств ЗИ в телекоммуникационных системах и сетях. Уметь: проводить анализ угроз, рисков ТКС, осуществлять выбор оборудования и средств защиты ТКС в соответствии с решаемыми ТКС задачами. Владеть навыками: анализа функциональных возможностей оборудования и средств защиты ТКС. Знать: требования действующих	разработки служебной и технической документации. Знать: перечень и объём мероприятий по обеспечению безопасности и защищённости ТКС, виды угроз ТКС, типы, виды, назначение средств защиты информации в ТКС. Уметь: классифицировать средства защиты исходя из функционала ТКС, определять состав средств защиты для обеспечения выполнения задач ТКС. Владеть навыками: проведения анализа технических характеристик сетевого оборудования и программно-аппаратных средств ЗИ в ТКС. Знать: классификацию общих критериев, пути организации	программных средств защиты информации, разработки архитектуры сетевой защиты, методами, методиками и моделями оценки функционирования программно-аппаратных средств защиты информации. Знать: состав, характеристики, назначение, функции оборудования ТКС; классификацию антивирусного ПО, способы настройки сетевых экранов. Уметь: применять программные средства защиты сетевого оборудования, антивирусные программные комплексы, настраивать режимы работы межсетевых экранов. Владеть навыками: выбора и эксплуатации средств ЗИ в ТКС в соответствии с функциональными задачами ТКС, настройки сетевых экранов, установки ПО, разработки защищённых сайтов. Знать: ; основные принципы построения политики

	ых в телекоммуникационных системах. ПК-3.4 Формулирует предложения по повышению эффективности механизмов безопасности, используемых в телекоммуникационных системах.	стандартов и рекомендаций, определяющих критерии оценки эффективности механизмов безопасности телекоммуникационных систем и этапы анализа рисков и угроз безопасности и уязвимости ТКС. Уметь: применять требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС. Владеть навыками: навыками применения требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС. Знать: классификацию, назначение, конфигурацию, состав, структуру, принципы функционирования типовых телекоммуникационных систем предприятий и организаций; основы управления ТКС. Уметь: проводить	общих критериев; требования к разработке должностных инструкций; порядок эксплуатации программно-аппаратных средств защиты ТКС. Уметь: разрабатывать служебную и техническую документацию; применять средства защиты информации в соответствии с заданными требованиями к ТКС. Владеть навыками: разработки служебной и технической документации; программных средств защиты информации. Знать: виды, состав, назначение, принципы функционирования, функции и взаимосвязь основных элементов и компонентов ТКС; понятие, типы, примеры архитектур ТКС, принципы работы ТКС; типовые архитектуры ТКС с точки зрения	безопасности; методы и способы защиты информации в ТКС, методы анализа угроз и оценки рисков информационной безопасности ТКС. Уметь: проводить анализ информационных рисков и эффективности, применяемых СЗИ в ТКС. Владеть навыками: формулирования требований к отдельным модулям, проектируемой ЗИС. Знать: распределённые системы; особенности проектирования распределённых систем; методы и средства защиты информации в ТКС, способы защиты информационных систем, методы анализа угроз и оценки рисков информационной безопасности ТКС. Уметь: разрабатывать регламентирующие

		сравнительный анализ состава, технических характеристик, решаемых задач компонентов ИС прикладного характера, системного и прикладного ПО, обеспечивающего функционирование ТКС; оценку вариантов предлагаемых к реализации архитектур ТКС. Владеть навыками: оценки предлагаемых к реализации вариантов построения телекоммуникационных систем, выбора оптимальной архитектуры прикладной ТКС исходя из решаемых системой задач.	программно-аппаратной реализации; классификацию архитектур. Уметь: выбор наиболее оптимального варианта построения предлагаемой архитектуры ТКС; формировать требования к структуре ТКС исходя из решаемых задач. Владеть навыками: разработки и оформления документов и предложений по повышению эффективности применения средств безопасности телекоммуникационных систем.	документы для принятия решения на технических совещаниях; предложения для технических советов с обоснованием выбора предлагаемой архитектуры прикладной ТКС. Владеть навыками: сравнительного анализа технических средств и оборудования из состава телекоммуникационных систем.
ПК-4, завершающий.	ПК-4.1 Разрабатывает проектные документы на средства защиты информации и создаваемых телекоммуникационных систем и сетей.	Знает: сетевой график проведения работ в рамках проекта, технологический цикл проведения разработок, состав материально технической и лабораторной базы необходимой для разработки программно-аппаратных средств, сборки и монтажа сетевого оборудования ТКС. Умеет: управлять материальными,	Знает: порядок разработки и согласования расчётно-калькуляционных материалов проекта по разработке ТКС. Умеет: управлять инструментами и оборудованием необходимыми для выполнения работ по проектированию ТКС. Владеет: Навыками управления инструментами и оборудованием	Знает: состав и структуру планово-хозяйственных документов, финансовых документов, отчётных документов, порядок их оформления, программные продукты и системы управления хозяйственной деятельностью. Умеет: управлять материальными, нематериальными,

		нематериальными, финансовыми ресурсами. Владеет: Навыками управления и распределения материальными, нематериальными, финансовыми ресурсами.	необходимыми для выполнения работ по проектированию ТКС.	финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию ТКС. Владеет: навыками управления и распределения материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию ТКС.
	ПК-4.2 Готовит техническую и проектную документацию по вопросам создания и эксплуатации телекоммуникационных систем и сетей. ПК-4.3 Проводит аттестацию программ и алгоритмов на предмет	Знает: Компоненты системы, порядок внедрения, отладки и развития процессов и этапов разработки требований к ТКС. Умеет: организовать и управлять внедрением, отладкой и развитием процессов и этапов работ. Владеет: навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности ТКС в процессе их разработки и эксплуатации. Знает:	Знает: задачи, критерии качества и методы обеспечения информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации. Умеет: применять методы обеспечения информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации. Владеет: Навыками применять методов обеспечения информационной безопасности защищённых ТКС в процессе их разработки и эксплуатации. Знает: основные виды сетевых атак и методы противодействия им, требования к	Знает: Нормативные требования и руководящие документы для разработки технической и проектной документации по созданию и эксплуатации ТКС. Умеет: использовать нормативные требования и руководящие документы для разработки технической и проектной документации по созданию и эксплуатации ТКС. Владеет: Навыками разработки технической и проектной документации по созданию и

	соответствия требованиям защиты информации. ПК-4.4 Производит сравнительный анализ вариантов конфигураций и состава телекоммуникационных систем и сетей.	виды угроз и возможные каналы утечки информации, основные принципы построения политики информационной безопасности. Умеет: применятьметоды и способы разработки алгоритмов, программных средств и комплексов защиты информации в ТКС. Владеет: навыками применения программных средств защиты информации. Знать: номенклатуру современных программно-аппаратных средств	средствам защиты информации и защищённым системам и сетям. Умеет: эксплуатировать антивирусные программные комплексы, снижать вероятность отрицательных последствий сетевых атак путем правильной настройки операционной системы. Владеет: навыками разработки защищенных сайтов, разработки архитектуры инфо-коммутационных систем и сетевой защиты, поиска и обнаружения уязвимых узлов инфо-коммуникационных систем и сетей. Знать: механизмы защиты программно-аппаратных средств ТКС; классификацию и архитектуру ТКС; основные этапы аудита безопасности информационных	эксплуатации ТКС. Знает: технические характеристики, особенности установки и функционирования программных средств и комплексов защиты телекоммуникационных сетей и систем, средства разработки алгоритмов функционирования СЗИ ТКС. Умеет: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить анализ алгоритмов и программных средств защиты информации на предмет соответствия требованиям защищённых ТКС. Владеет: навыками анализа алгоритмов и программных средств защиты информации на предмет соответствия требованиям защищённых ТКС,разработки алгоритмов, программных средств и комплексов защиты информации в ТК.

		телекоммуникационных систем и сетей; назначение, организацию и принципы функционирования программно-аппаратных средств ТКС. Уметь: устанавливать современные программные средства, подключать аппаратные средства ТКС. Владеть навыками: применения программно-аппаратных средств; реализации требуемых политик безопасности с помощью современных программно-аппаратных средств защиты информации.	систем; методы анализа и управления рисками; основные требования к системам защиты информации. Уметь: настраивать операционные системы и их подсистемы; сопоставлять структурную организацию программных и аппаратных средств требованиям политики безопасности; проводить анализ угроз, рисков, применять антивирусные программные комплексы, настраивать режимы работы межсетевых экранов, проводить анализ защищенности локальной вычислительной сети, проводить анализ информационных рисков. Владеть навыками: проведения проверок работоспособности и эффективности применения программно-аппаратных средств, защиты информации в компьютерных системах.	Знать: показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности ТКС; основные этапы сравнительного анализа состава и конфигурации ТКС, в том числе номенклатуру покупных и вновь разрабатываемых программных и аппаратных средства ТКС. Уметь: проводить основные этапы сравнительного анализа состава и конфигурации ТКС, в том числе покупных и вновь разрабатываемых программных и аппаратных средств ТКС. Владеть навыками: анализа защищенности ТКС, эксплуатации программных и аппаратных средств; проведения основных этапов сравнительного анализа состава и конфигурации ТКС, в том числе покупных и вновь разрабатываемых программных и аппаратных средств ТКС.

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

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные аспекты построения системы информационной безопасности.	УК-2, УК-6, ПК-3, ПК-4	Лекция, практическая работа, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
				КВЗПР №1	1-4	
2	Мероприятия по защите информации.	УК-2, УК-6, ПК-3, ПК-4	Лекция, практическая работа, СРС	Вопросы для устного опроса	11-20	Согласно таблице 7.2
				КВЗПР №2	1-4	
3	Требования к архитектуре ТКС для обеспечения безопасности ее функционирования.	УК-2, УК-6, ПК-3, ПК-4	Лекция,практическая работа, СРС	Вопросы для устного опроса	21-31	Согласно таблице 7.2
				КВЗПР №3	1-4	
4	Оценочные стандарты и	УК-2, УК-6,	Лекция, лаборатор	Вопросы для устного опроса	32-42	Согласно таблице 7.2

	технические спецификации.	ПК-3, ПК-4	ная работа, СРС	КВЗЛР №1	1-4	
5	Критерии оценки безопасности информационных технологий.	УК-2, УК-6, ПК-3, ПК-4	Лекция, лабораторная работа, СРС	Вопросы для устного опроса КВЗЛР №2	43-51 1-4	Согласно таблице 7.2
6	Руководящие документы ФСТЭК России.	УК-2, УК-6, ПК-3, ПК-4	Лекция, практическая работа, лабораторная работа, СРС	Вопросы для устного опроса КВЗПР №4, КВЗЛР №3	52-60 1-4 1-4	Согласно таблице 7.2

СРС – самостоятельная работа студента,

КВЗЛР – контрольные вопросы для защиты лабораторных работ,

КВЗПР – контрольные вопросы для защиты практических работ

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы дляустного опроса по разделу (теме) 5. «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?
6. Что такое уровни доверия?
7. Какие существуют механизмы обеспечения безопасности в распределённых системах?

Контрольные вопросы для защиты лабораторной работы №2:

Определение показателей защищенности информации при несанкционированном доступе.

1. В чем заключаются основные принципы проектирования защищённых систем?

2. Перечислите показатели качества процесса проектирования.

3. Постановка проблемы комплексного обеспечения информационной безопасности защищённых систем.

4. Основы методологии многовариантного планирования процесса проектирования.

5. Методы и методики проектирования комплексных систем информационной безопасности от несанкционированного доступа.

6. Методы и методики оценки качества комплексных систем информационной безопасности.

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 зачёта.

Промежуточная аттестация по дисциплине проводится в формезачёта.Зачёт проводится в виде бланкового 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 проведенияпромежуточной аттестации обучающихся

Задание в закрытой форме:

1. Руководитель, оценивая результаты создания системы безопасности, прежде всего, должен обратить внимание на:

А) Экономический эффект от внедрения системы.

Б) Функциональную полноту, адаптивность, корректность работы системы.

В) Эффективность использования системой существующей инфраструктуры.

Г) Степень достижения поставленных целей.

Задание в открытой форме:

1. Элементом архитектуры системы безопасности организации является…….

2. Архитектура информационных систем организации включает в себя……..

3. Формальное описание архитектуры предприятия впервые былосформулированов……...

4. В системном проектировании существуют следующие уровни представленияархитектуры……

Задание на установление правильной последовательности.

Установите последовательность этапов проектирования и разработкизащищённой ИС:

1. Внедрение

2. Эксплуатация и модификация

3. Разработка

4. Выявление требований

Задание на установление соответствия:

между ИТ- ресурсами защищённой ИС и описаниями функционированияеё элементов

1	Информация	А	Автоматизированные пользовательские системы, которые собирают, хранят, обрабатываютираспространяют информацию
2	Инфраструктура	Б	Данные во всех формах ввода, хранения,обработки и вывода с помощью информационных систем, в любыхформах, которые используются для принятия управленческихрешений
3	Персонал	В	Средства (аппаратное и программное обеспечение, системы управления базами данных, сеть, мультимедиа, среда, в которой все это функционирует), которые делают возможным работу приложений
4	Приложения	Г	Люди (специалисты), требующиеся для планирования, организации, установки, эксплуатации и развития информационных систем и сервисов, нанимаемые по контрактам

Компетентностно-ориентированная задача:

Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.

С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 100 узлов.

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 02.016–2018 Обалльно-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
1	2	3	4	5
Практическая работа № 1 «Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение»	6	Доля правильных ответов от 50% до 90%	12	Доля правильных ответов более 90%
Практическая работа № 2«Определение показателей защищенности информации при несанкционированном доступе»	6	Доля правильных ответов от 50% до 90%	12	Доля правильных ответов более 90%
Практическая работа № 3«Критерии оценки и выбора CASE-средств»	6	Доля правильных ответов от 50% до 90%	12	Доля правильных ответов более 90%

Практическая работа № 4«Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»	6	Выполнил, доля правильных ответов от 50% до 90%	12	Выполнил,доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	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 –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 за тестирование –36 баллов.

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

8.1 Основная учебная литература

1. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 «Информационная безопасность», 400301 «Юриспруденция», 380301 «Экономика»] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. : ил., табл. - Библиогр.: с. 188-195. - ISBN 978-5-7681-1196-0 : 290.00 р. - Текст : непосредственный.

2. Проскуряков, А. В. Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В.

Проскуряков ; Министерство науки и высшего образования Российской Федерации ; Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» ; Инженерно-технологическая академия. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 202 с.: ил. - URL: http://biblioclub.ru/index.php?page=book&id=561238.(дата обращения 02.09.2021) . - Режим доступа : по подписке. – Текст : электронный.

3. Горбунов, А. В. Проектирование защищённых оптических телекоммуникационных систем : учебное пособие / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. - Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. - 128 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=598665 (дата обращения 02.09.2021) . - Режим доступа: по подписке. - Библиогр.: с. 116 - 120. - ISBN 978-5-9275-3431-9. - Текст : электронный.

8.2 Дополнительная учебная литература

4. Безбогов, А. А. Методы и средства защиты компьютерной информации : учебное пособие / А. А. Безбогов, А. Я. Яковлев, В. Н. Шамкин. - Тамбов : ТГТУ, 2006. - 196 с. – Режим доступа:http://window.edu.ru/resource/546/38546. – Текст : электронный.

5. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для студентов вузов, обучающихся по направлению 552800 "Информатика и вычислительная техника" и по специальностям 220100 "Вычислительные машины, комплексы, системы и сети", 220200 "Автоматизированные системы обработки информации и управления" и 220400 "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Г. Олифер, Н. А. Олифер. - 5-е изд. - Санкт-Петербург : Питер, 2019. - 922 с. – Текст : непосредственный.

6. Грибунин, В. Г. Комплексная система защиты информации на предприятии : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М. : Академия, 2009. - 416 с. – Текст : непосредственный.

7. Аверченков, В. И. Служба защиты информации: организация и управление : [16+] / В. И. Аверченков, М. Ю. Рытов. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 186 с.– URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 02.09.2021). – Режим доступа : по подписке. - Текст : электронный.

8. Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл.–

URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 02.09.2021). – 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. - Курск : ЮЗГУ, 2017. - 16 с.

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. - Курск : ЮЗГУ, 2017. - 7 с.

3. Критерии оценки и выбора CASE-средств [Электронный ресурс] : методические указания по выполнению практических работ по дисциплине «Проектирование защищенных телекоммуникационных систем» для студентов специальности 10.05.02 / Юго-Зап. гос. ун-т; сост.: А. Л. Марухленко. – Курск : ЮЗГУ, 2017. - 10 с.

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. - Курск : ЮЗГУ, 2017. - 7 с.

5. Разработка проекта локальной вычислительной сети предприятия [Электронный ресурс] : методические указания по выполнению лабораторных работ по дисциплине «Проектирование защищенных телекоммуникационных систем» для студентов специальности 10.05.02 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 10 с.

6. Устранение уязвимостей сетевых портов [Электронный ресурс] : методические указания по выполнению лабораторных работ по дисциплине «Проектирование защищенных телекоммуникационных систем» для студентов специальности 10.05.02 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 10 с.

7. Изучение механизмов безопасности сетей Wi-Fi [Электронный ресурс] : методические указания по выполнению лабораторных работ по дисциплине «Проектирование защищенных телекоммуникационных систем»

для студентов специальности 10.05.02 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 10 с.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца
2. Журнал «InformationSecurity/Информационная безопасность.»- http://window.edu.ru/
3. Журнал «Проблемы информационной безопасности. Компьютерные системы»- http://window.edu.ru/
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность.»

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

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. http://microsoft.com - Корпорация Microsoft[официальный сайт].
8. http://www.consultant.ruКомпания«Консультант Плюс» [официальный сайт].

10. Методические указания дляобучающихся поосвоениюдисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Управление разработкой систем безопасности» являются лекциии практические 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 практические занятия, 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.

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.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Управление разработкой систем безопасности»: 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 лекций, участие в групповых и индивидуальных консультациях (собеседованиях). 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 закрепления 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 «Управление разработкой систем безопасности» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Управление разработкой систем безопасности» - 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)

MicrosoftOffice 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

Антивирусная программа Kaspersky Internet Security.

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 (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут-букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проекторinFocusIN24+

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
	Изме-нённых	Заменённых	Аннулированных	новых			
