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 информационных систем.

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;

Компетенции, формируемые в результате освоения дисциплины

Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий(УК-1)

Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели (УК-3)

Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки (УК-6)
Способен формировать проектные решения по созданию и модернизации защищённых информационных систем (ПК-1)
Способен проводить теоретические и экспериментальные исследования защищённости информационных систем (ПК-3)
Способен управлять персоналом, обслуживающим защищённые информационные системы (ПК-6)

Разделы дисциплины

Основные аспекты построения системы информационной безопасности. Требования к архитектуре ИС для обеспечения безопасности ее функционирования. Оценочные стандарты и технические спецификации. Критерии оценки безопасности информационных технологий. уководящие 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 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление разработкой систем безопасности

(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Защищённые информационные системы»
наименование направленности (профиля, специализации)

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

Курск – 2021

Рабочая программа дисциплины Управление разработкой систем безопасности составлена в соответствии с ФГОС ВО – магистратура по направлению подготовки (специальности) 10.04.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, направленность Защищённые информационные системы, 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 10.04.01 Информационная безопасность, направленность Защищённые информационные системы на заседании кафедры информационной безопасности Протокол № 1 «20» 01 2021 г.

Зав. кафедрой Таныгин М.О.
Разработчик программы
к.воен.н., доцент Ханис А.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 10.04.01 Информационная безопасность, направленность Защищённые информационные системы, одобренного Ученым советом университета Протокол № 7 «26» 02 2021 г., на заседании кафедры ИБ №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 10.04.01 Информационная безопасность, направленность Защищённые информационные системы, одобренного Ученым советом университета Протокол № 7 «29» 02 2022 г., на заседании кафедры ИБ протокол №1 от 30.08.2022.

(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 модернизации защищённых информационных систем.

1.2 Задачи 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;
- анализ проблемных ситуаций на основе системного и междисциплинарных подходов.

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-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	УК-1.4 Разрабатывает и аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.	***Знать:*** принципы построения защищённых систем, методы и средства защиты операционных систем, сетевого оборудования, управления доступом, идентификации и аутентификации, настройки межсетевых экранов, защиты от компьютерных вирусов, вопросы организации системы защиты информации в информационных системах (ИС), этапы построения системы защиты информации, политики безопасности, виды угроз и возможные каналы утечки информации, основы проектирования и построения архитектур систем безопасности, методы, модели и технологии проектирования систем безопасности, требования стандартов и руководящих документов, стадии и этапы создания систем безопасности. ***Уметь:*** правильно 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. ***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.
УК-3	Способен организовывать и руководить работой ко-	УК-3.1 Вырабатывает стратегию со-	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пуско-наладочных работ; тре-

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*		
	манды, вырабатывая командную стратегию для достижения поставленной цели.	трудничества и на её основе организует отбор членов команды для достижения поставленной цели.	бования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками организации, распределения, контроля и выполнения задач по проектированию ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.
		УК-3.2 Планирует и корректирует работу команды с учётом интересов, особенностей поведения и мнений её членов.	***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 защищённых ИС, этапы разработки типовой прикладной ИС, 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

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*		
			информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем. ***Уметь***: организовать выполнение работ в рамках проекта по разработке прикладных ИС, 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 прикладных ИС, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других 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-3.3 Разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон.	***Знать:*** классификацию, назначение, конфигурацию, состав, структуру, принципы функционирования типовых защищенных ИС предприятий; основы управления ИС; виды, состав, назначение, принципы функционирования, функции и взаимосвязь основных элементов и компонентов ИС; понятие, типы, примеры архитектур ИС, принципы работы ИС; типовые архитектуры ИС с точки зрения программно-аппаратной реализации; классификацию архитектур; особенности проектирования распределённых систем; методы и средства защиты информации в ИС, способы защиты информационных систем, методы анализа угроз и оценки рисков информационной безопасности ИС.

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: проводить сравнительный анализ состава, технических характеристик, решаемых задач компонентов ИС прикладного характера, системного и прикладного ПО, обеспечивающего функционирование ИС; оценку вариантов предлагаемых к реализации архитектур ИС; выбор наиболее оптимального варианта построения предлагаемой архитектуры ИС; формировать требования к структуре ИС исходя из решаемых задач; разрабатывать регламентирующие документы для принятия решения на технических совещаниях; предложения для технических советов с обоснованием выбора предлагаемой архитектуры прикладной ИС. ***Владеть:*** навыками сравнительного анализа технических средств и оборудования из состава прикладных ИС, оценки предлагаемых к реализации вариантов построения прикладных ИС, выбора оптимальной архитектуры прикладной ИС исходя из решаемых системой задач, разрешения конфликтных ситуаций в ходе выполнения работ по разработке защищённых ИС.
		УК-3.4 Организует дискуссии по заданной теме и обсуждение результатов работы команды с привлечением оппонентов разработанным идеям	***Знать:*** порядок внедрения, отладки и этапы разработки систем обеспечения информационной безопасности ИС. ***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС. ***Владеть:*** навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС, организации обсуждений результатов работы команды с привлечением оппонентов разработанным идеям в рамках создания защищённых ИС.
		УК-3.5	***Знать:*** нормативные документы и госты

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*		
		Планирует командную работу, распределяет поручения и делегирует полномочия членам команды.	по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пуско-наладочных работ; требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию защищённых ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками планирования, организации, распределения, контроля и выполнения задач исполнителями по проектированию защищённых ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.	УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения по-	***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

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*		
		рученного задания.	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.
ПК-1	Способен формировать проектные решения по созданию и модернизации защищённых информационных систем	ПК-1.1 Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей.	***Знать:*** Номенклатуру средств разработки телекоммуникационных систем и сетей. Принципы и средства разработки защищённых ИС, все этапы, методы и средства проектирования защищённых ИС. ***Уметь:*** Формулировать требования к защищённым ИС, реализовывать основные этапы обеспечения безопасности ИС, самостоятельно ставить задачи по обеспечению ИБ ИС, производить их декомпозицию. ***Владеть:*** Базовыми технологиями обеспечения информационной безопасности, основными методами обеспечения ИБ ИС.

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-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем.	***Знать:*** основные подходы к оценке качества защищённых ИС, методики проведения испытаний защищённых ИС, методологические аспекты для выявления соответствия характеристик защищённых ИС требованиям, к ним предъявляемым. ***Уметь:*** определять функциональные характеристики отдельных структурных компонентов ИС, определять на основе функционала компонентов защищённых ИС уровень защищённости системы в целом, самостоятельно разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности. ***Владеть:*** навыками анализа защищённых ИС и выявления характеристик, как всех систем в целом, так и их отдельных функциональных блоков.
		ПК-1.3 Сопоставляет характеристики проектируемых решений с требованиями защиты информации.	***Знать:*** Основные стандарты ИБ, структуру и содержание стандартов ИБ, структуру, содержание и методологические аспекты, лежащие в основе стандартов ИБ. ***Уметь:*** Соотносить требования стандартов ИБ реальным системам, сопоставлять требования стандартов к целым защищённым информационным системам и их отдельным структурным компонентам, обосновывать применение технологий ЗИ . ***Владеть:*** Навыками использования стандартов ИБ для классификации ИС, применения стандартов ИБ, оценки соответствия защищённых информационных систем требованиям стандартов.
		ПК-1.4 Формирует конфигурацию	***Знать:*** номенклатуру современных программно-аппаратных средств ИС; назначение, организацию и принципы функциони-

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*		
		и состав защищённых информационных систем.	ровании программно-аппаратных средств ИС; механизмы защиты программно-аппаратных средств ИС; классификацию и архитектуру ИС; 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; типовой состав и конфигурации защищённых ИС, в том числе номенклатуру покупных и вновь разрабатываемых программных и аппаратных средств ИС. ***Уметь:*** устанавливать современные программные средства, подключать аппаратные средства ИС; 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; формировать состав и конфигурации защищённой ИС, в том числе покупных и вновь разрабатываемых программных и аппаратных средств ИС. ***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 ИС, эксплуатации программных

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*		
			и аппаратных средств; формирования состава и конфигурации защищённой ИС, в том числе покупных и вновь разрабатываемых программных и аппаратных средств ИС.
ПК-3	Способен проводить теоретические и экспериментальные исследования защищённости информационных систем.	ПК-3.2 Разрабатывает формальные модели обработки и передачи данных в информационных системах.	***Знать:*** основные подходы к оценке качества защищённых ИС, методики проведения теоретических и экспериментальных исследований защищённости ИС, методологические аспекты для выявления соответствия характеристик защищённых ИС требованиям, к ним предъявляемым. ***Уметь:*** определять функциональные характеристики отдельных структурных компонентов ИС, определять на основе функционала компонентов защищённых ИС уровень защищённости системы в целом, самостоятельно разрабатывать программы и методики проведения теоретических и экспериментальных исследований средств и систем обеспечения информационной безопасности. ***Владеть:*** навыками анализа защищённых ИС и выявления характеристик, как всех систем в целом, так и их отдельных функциональных блоков, разработки технического облика средств обработки и передачи данных в информационных системах, разработки методик теоретических и экспериментальных исследований защищённости информационных систем.
ПК-6	Способен управлять персоналом, обслуживающим защищённые информационные системы	ПК-6.1 Формирует цели, приоритеты, обязанности и полномочия персонала, обслуживающего информа-	***Знать:*** требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру, архитектуру и состав типовых защищённых ИС, этапы разработки типовой прикладной ИС, сетевой график

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*		
		ционные системы.	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 защищённых ИС, 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 защищённых ИС, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов; своевременного внесения корректив в разработанную документацию и устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов.
		ПК-6.2 Формулирует трудовые задачи при проведении работ по развитию, модернизации защищённой информацион-	***Знать:*** порядок внедрения, отладки и развития процессов и этапов разработки требований, задач, критериев качества и методов обеспечения информационной безопасности защищённых ИС в процессе их эксплуатации и модернизации. ***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессов и этапов работ, методов обеспечения ин-

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*		
		ной системы.	формационной безопасности защищённых ИС в процессе их эксплуатации и модернизации. ***Владеть:*** навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности ИС в процессе их эксплуатации и модернизации.
		ПК-6.3 Формирует требования, предъявляемые потребителями к программным, программно-аппаратным и техническим средствам и системам защиты информации.	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации, основные принципы построения политики информационной безопасности, основные виды сетевых атак и методы противодействия им. ***Уметь:*** правильно 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. ***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.
		ПК-6.4 Определяет порядок действий проведении процедур сертификации и аттестации средств и систем защиты и объектов информатизации.	***Знать:*** Основные стандарты ИБ, структуру и содержание стандартов ИБ, структуру, содержание и методологические аспекты, лежащие в основе стандартов ИБ. ***Уметь:*** Соотносить требования стандартов ИБ реальным системам, сопоставлять требования стандартов к целым защищённым информационным системам и их отдельным структурным компонентам, обосновывать

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*		
			применение технологий ЗИ . ***Владеть:*** Навыками использования стандартов ИБ для классификации ИС, применения стандартов ИБ, оценки соответствия защищённых информационных систем требованиям стандартов.
		ПК-6.5 Формирует отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации.	***Знать:*** номенклатуру организационно-распорядительной документации службы информационной безопасности, состав организационно-распорядительной документации службы информационной безопасности, назначение и правовые основы отдельных положений организационно-распорядительной документации службы информационной безопасности. ***Уметь:*** сопоставлять организационно-распорядительную документацию с функциями службы информационной безопасности, требованиям нормативных документов, актуальной структуре предприятия. ***Владеть:*** Навыками применения требований нормативных правовых актов, руководящих и методических документов, предъявляемых к системам защиты информации, стандартов ИБ для классификации защищённых ИС, применения стандартов ИБ, оценки соответствия защищённых информационных систем требованиям стандартов, разработки отчётной документации по изменениям в нормативной и организационно-распорядительной документации.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Управление разработкой систем безопасности», входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули)») основной профессиональной образовательной программы – программы магистратуры (специалитета, бакалавриата) 10.04.01 Информационная безопасность, направленность Защищённые информационные системы. Дисциплина изучается на 2 курсе в 3 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 5 зачетных единиц (з.е.), 180 академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	90
в том числе:	
лекции	36
лабораторные занятия	0
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 информационной безопасности.
2	Мероприятия по защите информации.	Нормативно-законодательный аспект. Процедурный аспект. Программно-технический аспект.
3	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.
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 ИС, 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-1, УК-3, УК-6, ПК-1, ПК-3
2	Мероприятия по защите информации.	6	-	2	У-1-3, МУ-2	УО – 4, ЗПР – 4	УК-1, УК-3, УК-6, ПК-1, ПК-3

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

УО – устный опрос, ЗПР – защита практической работы

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические 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 информации при 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;

путем разработки:

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

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

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

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Современная философия и методология науки. Организация работ по обеспечению безопасности в информационных системах.	Организация работ по обеспечению безопасности в информационных системах.	Подготовка к процедуре защиты и защита выпускной квалификационной работы.
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	Управление информационной безопасностью.	Управление информационной безопасностью.	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.	Управление информационной безопасностью.	Управление информационной безопасностью.	Подготовка к процедуре защиты и защита выпускной квалификационной работы.
ПК-1. Способен формировать проектные решения по созданию и модернизации защищённых информационных систем.	Технологии распределенных реестров. Безопасность распределённых систем.	Методы и средства защиты информации в системах электронного документооборота. Теоретические основы компьютерной безопасности.	Методы и средства защиты информации в системах электронного документооборота. Теоретические основы компьютерной безопасности. Производственная проектно-технологическая практика. 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 проводить теоретические и экспериментальные исследования защищённости информационных систем.	Теоретические основы компьютерной безопасности.	Теоретические основы компьютерной безопасности.	Подготовка к процедуре защиты и защита выпускной квалификационной работы.
ПК-6. Способен управлять персоналом, обслуживающим защищённые информационные системы.	Методы и средства защиты информации в системах электронного документооборота.	Методы и средства защиты информации в системах электронного документооборота.	Производственная преддипломная 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 из п.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-1, завершающий.	УК-1.4 Разрабатывает и аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.	Знать: виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам. Уметь: выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации на объектах информатизации и вскрытия каналов утечки информации, по организации мероприятий, направленных на защиту информации. Владеть: навыками разработки нормативных и технических документов по организации защиты объекта информатизации.	Знать: основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения радиоволн, принципы и способы организации системы защиты информации на объектах информатизации. Уметь: разрабатывать нормативную документацию по выполнению требований защиты информации на объектах информатизации. Владеть: навыками применения технических средств защиты информации.	Знать: порядок и алгоритм проведения организационных мероприятий на объектах информатизации. Функциональные обязанности по организации мероприятий по защите информации. Уметь: осуществлять выбор технических средств защиты информации в зависимости от условий эксплуатации объектов информатизации. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. Владеть: навыками проведения организационных мероприятий по вскрытию уязвимых мест систем обеспечения защиты информации объекта информатизации.
УК-3, завершающий.	УК-3.1 Вырабатывает стратегию сотрудничества и на её основе организует отбор членов команды для достижения поставлен-	Знает: основные подходы к формированию политик информационной безопасности. Умеет: оформлять и представлять результаты описания процессов протекающих в информационных системах	Знает: сформированные, но содержащие отдельные пробелы знания законов, технологий, правил, приемов обработки результатов математических экспериментов. Умеет: способен обработать и представить	Знает: глубокие знания проблематики описания информационных процессов с точки зрения безопасности. Умеет: способен самостоятельно обработать, проанализировать и представить результаты формального

	ной цели.	формальным языком. Владеет: описания информационных потоков в информационных системах.	результат проведённого анализа информационной системы. Владеет: основными навыками теоретического анализа информационных систем на предмет защищённости.	описания информационных систем. Владеет: уверенно владеет навыками теоретического анализа информационных систем на предмет защищённости.
	УК-3.2 Планирует и корректирует работу команды с учётом интересов, особенностей поведения и мнений её членов.	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 системы. 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.
	УК-3.3 Разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон.	Знает: основные подходы к формированию политик информационной безопасности. Умеет: оформлять и представлять результаты описания процессов протекающих в информационных системах формальным языком. Владеет: описания инфор-	Знает: сформированные, но содержащие отдельные пробелы знания законов, технологий, правил, приемов обработки результатов математических экспериментов. Умеет: способен обработать и представить результат проведённого анализа информационной системы.	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

		мационных потоков в информационных системах.	Владеет: основными навыками теоретического анализа информационных систем на предмет защищённости.	навыками теоретического анализа информационных систем на предмет защищённости.
	УК-3.4 Организует дискуссии по заданной теме и обсуждение результатов работы команды с привлечением оппонентов разработанным идеям.	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 системы. 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.
	УК-3.5 Планирует командную работу, распределяет поручения и делегирует полномочия членам команды.	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 системы. Владеет: основными навыками теоретического анализа инфор-	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 за-

			мационных систем на предмет защищённости.	щищённости.
УК-6, завершающий.	УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания.	Знать: виды угроз и возможные каналы утечки конфиденциальной информации. Уметь: эксплуатировать антивирусные программные комплексы. Владеть: навыками применения программных средств защиты информации.	Знать: основные принципы построения политики информационной безопасности. Уметь: снижать вероятность отрицательных последствий сетевых атак путем правильной настройки операционной системы. Владеть: навыками разработки защищенных сайтов.	Знать: основные виды сетевых атак и методы противодействия им. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: разработки архитектуры сетевой защиты.
ПК-1, завершающий.	ПК-1.1 Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей.	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 функциональных возможностей компонентов ЗИС и требований политики безопасности. Владеть навыками: формулирования требований к отдельным модулям ,проектируемой ЗИС.
	ПК-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем.	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 требо-	Знать: принципы декомпозиции при определении функциональности блоков разрабатываемых систем. Уметь: анализ соответствия функциональных возможностей компонентов ЗИС и требований полити-

			ваний к отдельным модулям проектируемой ЗИС.	ки безопасности. Владеть навыками: формулирования требований к отдельным модулям, проектируемой ЗИС.
	ПК-1.3 Сопоставляет характеристики проектируемых решений с требованиями защиты информации.	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 функциональных возможностей компонентов ЗИС и требований политики безопасности. Владеть навыками: формулирования требований к отдельным модулям, проектируемой ЗИС.
	ПК-1.4 Формирует конфигурацию и состав защищённых информационных систем.	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 функциональных возможностей компонентов ЗИС и требований политики безопасности. Владеть навыками: формулирования требований к отдельным модулям, проектируемой ЗИС.

ПК-3, завершающий.	ПК-3.2 Разрабатывает формальные модели обработки и передачи данных в информационных системах.	Знать: терминологию предметной области информационной безопасности. Уметь: использовать различные подходы к классификации процессов в области ИБ. Владеть навыками: использования различных методологических подходов в анализе прикладных и фундаментальных задач информационной безопасности.	Знать: основные фундаментальные положения теории информационной безопасности . Уметь: сопоставлять фундаментальные теории информационной безопасности реальным процессам в информационных системах. Владеть навыками: анализа объекта исследования с точки зрения возможности описания протекающих в нём процессов формальным языком.	Знать: принципы организации защиты информации в РФ и мире. Уметь: проводить математический эксперимент и оценивать его достоверность. Владеть навыками: проведения математического эксперимента.
ПК-6, завершающий.	ПК-6.1 Формирует цели, приоритеты, обязанности и полномочия персонала, обслуживающего информационные системы. ПК-6.2 Формулирует трудовые задачи при проведении работ по развитию, модернизации защищённой информационной системы.	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: 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: Навыками конфигурирования ЗИС для обеспечения требуемого качества и функционала. Знает: Жизненный цикл ИС Умеет: Организовывать реализацию жизненного цикла ЗИС. Владеет: Навыками 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. Знает: Детальные аспекты жизненного цикла ИС. Умеет: Самостоятельно проводить оценку качества работы СЗИ. Владеет: Навыками организации работ по вводу в эксплуатацию СЗИ.

	ПК-6.3 Формирует требования, предъявляемые потребителями к программным, программно-аппаратным и техническим средствам и системам защиты информации.	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: Навыками 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.
	ПК-6.4 Определяет порядок действий проведении процедур сертификации и аттестации средств и систем защиты и объектов информатизации.	Знать: номенклатуру организационно-распорядительной документации службы информационной безопасности. Уметь: сопоставлять организационно-распорядительную документацию с функциями службы информационной безопасности; Владеть навыками: Работы с технической документаций.	Знать: состав организационно-распорядительной документации службы информационной безопасности. Уметь: сопоставлять ОРД требованиям нормативных документов Владеть навыками: Формулирования отдельных положений ОРД.	Знать: назначение и правовые основы отдельных положений организационно-распорядительной документации службы информационной безопасности. Уметь: сопоставлять ОРД актуальной структуре предприятия; Владеть навыками: Формирования ОРД.
	ПК-6.5 Формирует отчёты по изменению за выбранный период времени требований нормативных правовых актов, руководящих и методических документов,	Знать: номенклатуру организационно-распорядительной документации службы информационной безопасности Уметь: сопоставлять организационно-распорядительную документацию с функциями службы информацион-	Знать: состав организационно-распорядительной документации службы информационной безопасности Уметь: сопоставлять ОРД требованиям нормативных документов Владеть навыками: Формулирования	Знать: назначение и правовые основы отдельных положений организационно-распорядительной документации службы информационной безопасности. Уметь: сопоставлять ОРД актуальной структуре предприятия; Владеть навыками: Формирования ОРД.

	предъявляемых к системам защиты информации.	ной безопасности; Владеть навыками: Работы с технической документаций.	отдельных положений ОРД.	

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

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или 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-1, УК-3, УК-6, ПК-1, ПК-3	Лекция, СРС	Вопросы для устного опроса КВЗЛР №1	1-10 1-4	Согласно таблице 7.2
2	Мероприятия по защите информации.	УК-1, УК-3, УК-6, ПК-1, ПК-3	Лекция, СРС	Вопросы для устного опроса КВЗЛР №2	11-20 1-4	Согласно таблице 7.2
3	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	УК-1, УК-3, УК-6, ПК-1, ПК-3	Лекция, СРС	Вопросы для устного опроса КВЗЛР №3	21-31 1-4	Согласно таблице 7.2
4	Оценочные стандарты и технические спецификации.	УК-1, УК-3, УК-6, ПК-1, ПК-3, ПК-6	Лекция, СРС	Вопросы для устного опроса	32-42	Согласно таблице 7.2
5	Критерии оценки безопасности информационных	УК-1, УК-3, УК-6, ПК-1,	Лекция, СРС	Вопросы для устного опроса	43-51	Согласно таблице 7.2

	технологий.	ПК-3, ПК-6				
6	Руководящие документы ФСТЭК России.	УК-1, УК-3, УК-6, ПК-1, ПК-3, ПК-6	Лекция, СРС	Вопросы для устного опроса КВЗЛР №4	52-60 1-4	Согласно таблице 7.2

СРС – самостоятельная работа студента,

КВЗПР – контрольные вопросы для защиты практических работ,

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного 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 форме зачёта. 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 проведения промежуточной 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 было сформулировано в……...

4. В системном проектировании существуют следующие уровни представления архитектуры ……

Задание на установление правильной последовательности.

Установите последовательность этапов проектирования и разработки защищённой ИС:

1. Внедрение

2. Эксплуатация и модификация

3. Разработка

4. Выявление требований

Задание на установление соответствия:

между ИТ- ресурсами защищённой ИС и описаниями функционирования её элементов

1	Информация	А	Автоматизированные пользовательские системы, которые собирают, хранят, обрабатывают и распространяют информацию
2	Инфраструктура	Б	Данные во всех формах ввода, хранения, обработки и вывода с помощью информационных систем, в любых формах, которые используются для принятия управленческих решений
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 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
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 [Электронный ресурс] : учебное пособие / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. - Ростов-на-Дону ; Таганрог : Юж-

ный федеральный университет, 2019. - 128 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=598665.

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 [Текст] : 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 [Текст] : 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.

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. Компью терные 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.ru Компания «Консультант Плюс» [официальный сайт].

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Управление разработкой систем безопасности» являются лекции и 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)

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
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 (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 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
	Изменённых	Заменённых	Аннулированных	новых			